

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**

**版权所有 侵权必究**

凡购买铁道版的图书，如有缺页、倒页、脱页者，请与本社计算机图书批销部调换。

# 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者和计算机维护人员,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理事会理事 薛万奉  
上海市计算机基础教育协会理事

2006年7月

# 目 录

<b>第 1 章 计算机信息系统安全概述</b> .....	1
1.1 计算机信息系统及其安全的基本概念 .....	1
1.1.1 计算机信息系统 .....	1
1.1.2 计算机信息系统安全 .....	2
1.2 计算机信息系统面临的威胁及其脆弱性 .....	4
1.2.1 计算机信息系统面临的威胁 .....	4
1.2.2 计算机信息系统受到的威胁和攻击 .....	7
1.2.3 计算机信息系统的脆弱性 .....	9
1.3 计算机信息系统安全保护概述 .....	11
1.3.1 计算机信息系统安全保护的基本概念 .....	12
1.3.2 计算机信息系统保护的基本目标和任务 .....	15
1.4 我国计算机信息系统安全保护的基本政策 .....	17
1.4.1 我国信息化建设的总指导方针 .....	17
1.4.2 计算机信息系统保护的基本原则 .....	18
1.4.3 我国信息系统安全保护的总政策 .....	19
1.5 计算机安全监察 .....	21
1.5.1 计算机信息系统的安全监督检查的总体目标 .....	21
1.5.2 计算机安全监察工作指导方针 .....	22
1.5.3 实施安全监督检查 .....	22
1.5.4 计算机安全监察的业务范围 .....	23
思考题 .....	24
<b>第 2 章 信息论与数学基础</b> .....	25
2.1 信息论 .....	25
2.1.1 熵和不确定性 .....	25
2.1.2 语言信息率 .....	26
2.1.3 密码体制的安全性 .....	26
2.1.4 唯一解距离 .....	27
2.1.5 信息论的运用 .....	27
2.1.6 混乱和散布 .....	28
2.2 复杂性理论 .....	28
2.2.1 算法的复杂性 .....	28
2.2.2 问题的复杂性 .....	29
2.2.3 NP—完全问题 .....	30
2.3 数论 .....	30

2.3.1	模运算 .....	30
2.3.2	素数 .....	32
2.3.3	最大公因子 .....	32
2.3.4	取模数求逆元 .....	33
2.3.5	费马小定理 .....	33
2.3.6	欧拉函数 .....	33
2.3.7	中国剩余定理 .....	33
2.3.8	二次剩余 .....	34
2.3.9	勒让德符号 .....	34
2.3.10	雅可比符号 .....	35
2.3.11	Blum 整数 .....	35
2.3.12	生成元 .....	36
2.3.13	有限域 .....	37
2.3.14	$GF(p^m)$ 上的计算 .....	37
2.4	因子分解 .....	38
2.4.1	因子分解算法 .....	38
2.4.2	模 $n$ 的平方根 .....	39
2.5	素数生成元 .....	39
2.5.1	Solovag-Strassen 方法 .....	40
2.5.2	Rabin-Miller 方法 .....	40
2.5.3	Lehmann 方法 .....	41
2.5.4	强素数 .....	41
2.6	有限域上的离散对数 .....	41
2.6.1	离散对数基本定义 .....	41
2.6.2	计算有限群中的离散对数 .....	42
	思考题 .....	42
<b>第 3 章</b>	<b>信息加密技术与应用 .....</b>	<b>43</b>
3.1	网络通信中的加密方式 .....	43
3.1.1	链路-链路加密 .....	43
3.1.2	节点加密 .....	44
3.1.3	端-端加密 .....	45
3.1.4	ATM 网络加密 .....	45
3.1.5	卫星通信加密 .....	46
3.1.6	加密方式的选择 .....	46
3.2	分组加密与高级加密标准 .....	47
3.2.1	分组密码与 DES .....	47
3.2.2	21 世纪高级加密标准 .....	51

3.3 公钥加密体制.....	55
3.3.1 RSA 加密体制.....	56
3.3.2 背包加密体制.....	58
3.3.3 ElGamal 加密体制.....	59
3.4 复合型加密体制 PGP.....	59
3.4.1 完美的加密 PGP.....	60
3.4.2 PGP 的多种加密方式.....	60
3.4.3 PGP 的广泛使用.....	60
3.4.4 PGP 商务安全方案.....	61
3.5 微软的 CryptoAPI.....	62
3.6 对加密系统的计时入侵.....	64
3.7 加密新法: 椭圆曲线加密.....	65
3.8 加密产品与系统简介.....	66
思考题.....	66
<b>第 4 章 数字签名技术与应用.....</b>	<b>67</b>
4.1 数字签名的基本原理.....	67
4.1.1 数字签名的要求.....	67
4.1.2 数字签名与手书签名的区别.....	67
4.1.3 数字签名的分类.....	67
4.1.4 使用数字签名.....	68
4.2 RSA 签名.....	69
4.3 ElGamal 签名.....	69
4.4 盲签名及其应用.....	70
4.4.1 盲消息签名.....	70
4.4.2 盲参数签名.....	71
4.4.3 弱盲签名.....	72
4.4.4 强盲签名.....	72
4.5 多重签名及其应用.....	73
4.6 定向签名及其应用.....	73
4.6.1 ElGamal 型定向签名.....	74
4.6.2 MR 型定向签名方案.....	74
4.7 美国数字签名标准 (DSS).....	75
4.7.1 关注 DSS.....	75
4.7.2 NSA 的发展.....	75
4.7.3 DSS 的进展.....	77
4.8 世界各国数字签名立法状况.....	77
4.9 数字签名应用系统与产品.....	77
思考题.....	79



<b>第 5 章 黑客行径概述</b> .....	<b>80</b>
5.1 攻击的目的.....	80
5.1.1 进程的执行.....	80
5.1.2 获取文件和传输中的数据.....	80
5.1.3 获取超级用户的权限.....	80
5.1.4 对系统的非法访问.....	81
5.1.5 进行不许可的操作.....	81
5.1.6 拒绝服务.....	81
5.1.7 涂改信息.....	81
5.1.8 暴露信息.....	81
5.2 攻击类型 .....	82
5.2.1 口令攻击.....	82
5.2.2 社会工程.....	84
5.2.3 缺陷和后门.....	85
5.2.4 鉴别失败.....	89
5.2.5 协议失败.....	90
5.2.6 信息泄漏.....	90
5.2.7 拒绝服务.....	91
5.3 实施攻击的人员.....	91
5.3.1 计算机黑客.....	92
5.3.2 不满或被解雇的雇员.....	92
5.3.3 极端危险的罪犯和工业间谍.....	92
5.4 攻击的三个阶段.....	92
5.4.1 寻找目标, 收集信息.....	92
5.4.2 获得初始的访问权和特权.....	93
5.4.3 攻击其他系统.....	93
思考题 .....	93
<b>第 6 章 鉴别与防御“黑客”入侵</b> .....	<b>94</b>
6.1 最简单的“黑客”入侵.....	94
6.2 TCP 协议劫持入侵.....	95
6.3 嗅探入侵.....	96
6.4 主动的非同步入侵.....	97
6.4.1 非同步后劫持入侵.....	97
6.4.2 TCP ACK 风暴.....	99
6.4.3 前期非同步入侵.....	99
6.4.4 空数据非同步入侵.....	101
6.4.5 Telnet 会话入侵.....	101

---

---

6.4.6	进一步了解 ACK 风暴 .....	102
6.4.7	检测及其副作用 .....	102
6.5	另一种嗅探——冒充入侵 .....	103
6.6	关于作假的详述 .....	104
6.6.1	冒充 E-mail .....	105
6.7	关于劫持会话入侵 .....	105
6.7.1	检测劫持会话 .....	105
6.7.2	防卫劫持会话 .....	105
6.8	超级链接欺骗: SSL 服务器认证中的一种入侵 .....	105
6.8.1	超级链接欺骗的背景 .....	106
6.8.2	实施超级链接欺骗 .....	106
6.8.3	防卫超级链接欺骗的方法 .....	107
6.8.4	对超级链接欺骗的长远考虑 .....	108
6.9	网页作假 .....	109
6.9.1	网页作假的后果 .....	110
6.9.2	作假整个 Web .....	110
6.9.3	入侵过程 .....	110
6.9.4	重仿表格和安全连接 .....	111
6.9.5	开始网页作假入侵 .....	111
6.9.6	制造错觉——状态条 .....	112
6.9.7	位置行 .....	112
6.9.8	对网页作假入侵的补救措施 .....	113
6.9.9	对网页作假入侵的长远解决方案 .....	113
6.9.10	小结 .....	113
	思考题 .....	114
<b>第 7 章</b>	<b>入侵检测 .....</b>	<b>115</b>
7.1	入侵检测原理与技术 .....	115
7.1.1	入侵检测的起源 .....	115
7.1.2	入侵检测系统的需求特性 .....	116
7.1.3	入侵检测原理 .....	117
7.1.4	入侵检测分类 .....	118
7.1.5	入侵检测现状 .....	120
7.2	入侵检测的数学模型 .....	121
7.2.1	实验模型 .....	121
7.2.2	平均值和标准差模型 .....	121
7.2.3	多变量模型 .....	122
7.2.4	马尔可夫过程模型 .....	122

7.2.5	时序模型.....	122
7.3	入侵检测的特征分析和协议分析.....	122
7.3.1	特征分析.....	122
7.3.2	协议分析.....	125
7.4	入侵检测响应机制.....	126
7.4.1	对响应的需求.....	126
7.4.2	自动响应.....	127
7.4.3	蜜罐.....	128
7.4.4	主动攻击模型.....	128
7.5	绕过入侵检测的若干技术.....	129
7.5.1	对入侵检测系统的攻击.....	129
7.5.2	对入侵检测系统的逃避.....	130
7.5.3	其他方法.....	130
7.6	入侵检测标准化工作.....	130
7.6.1	CIDF 体系结构.....	131
7.6.2	CIDF 规范语言.....	132
7.6.3	CIDF 的通信机制.....	133
7.6.4	CIDF 程序接口.....	134
	思考题.....	134
<b>第 8 章</b>	<b>防火墙技术.....</b>	<b>135</b>
8.1	防火墙的基本概念.....	135
8.1.1	定义.....	135
8.1.2	防火墙结构.....	135
8.1.3	防火墙应满足的条件.....	135
8.1.4	防火墙的功能.....	136
8.1.5	防火墙的不足之处.....	136
8.2	防火墙的类型.....	136
8.2.1	类型.....	136
8.2.2	分组过滤路由器.....	136
8.2.3	应用级网关.....	137
8.2.4	电路级网关.....	137
8.3	防火墙的体系结构.....	138
8.3.1	双宿/多宿主机模式.....	138
8.3.2	屏蔽主机模式.....	139
8.3.3	屏蔽子网模式.....	139
8.4	防火墙的基本技术与附加功能.....	140
8.4.1	基本技术.....	140

8.4.2	附加功能.....	141
8.5	防火墙技术的几个新方向.....	142
8.5.1	透明接入技术.....	142
8.5.2	分布式防火墙技术.....	142
8.5.3	以防火墙为核心的网络安全体系.....	143
8.6	常见的防火墙产品.....	143
8.6.1	常见的防火墙产品.....	143
8.6.2	选购防火墙的一些基本原则.....	145
	思考题.....	145
<b>第9章</b>	<b>预防病毒.....</b>	<b>146</b>
9.1	病毒是如何工作的.....	146
9.2	最一般的传染威胁.....	147
9.2.1	一般的传染威胁.....	147
9.2.2	通过电子邮件传输病毒的威胁.....	148
9.3	病毒的类型.....	149
9.3.1	特洛伊木马.....	149
9.3.2	多态病毒.....	149
9.3.3	行骗病毒.....	149
9.3.4	慢效病毒.....	150
9.3.5	制动火箭病毒.....	151
9.3.6	多成分病毒.....	151
9.3.7	装甲病毒.....	151
9.3.8	同伴病毒.....	151
9.3.9	噬菌体病毒.....	152
9.3.10	回顾蠕虫事件.....	152
9.3.11	病毒对网络和 Internet 的威胁.....	152
9.3.12	关于文件病毒.....	152
9.4	关于宏病毒.....	153
9.4.1	一些流行的宏病毒.....	154
9.4.2	宏病毒的最佳解决办法.....	157
9.5	互联网上的病毒欺骗.....	158
9.5.1	IRINA 病毒.....	158
9.5.2	Good Times 病毒.....	158
9.5.3	a014free.com.....	158
9.5.4	怎样分辨出一个真正的病毒警告.....	159
9.6	防止病毒从 Internet 上感染你的网络.....	159
9.6.1	反病毒软件如何检测病毒.....	160

9.6.2 反病毒软件的主要出版商 .....	160
思考题 .....	161
<b>第 10 章 身份认证与访问控制 .....</b>	<b>162</b>
10.1 口令识别法 .....	162
10.1.1 用户识别方法分类 .....	162
10.1.2 不安全口令的分析 .....	163
10.1.3 一次性口令 .....	164
10.1.4 SecurID 卡系统 .....	165
10.2 个人特征识别 .....	165
10.2.1 机器识别 .....	166
10.2.2 系统误差 .....	166
10.3 签名识别法 .....	166
10.3.1 记录书写过程的技术 .....	167
10.3.2 签名识别法的使用 .....	167
10.4 指纹识别技术 .....	167
10.4.1 指纹识别技术简介 .....	168
10.4.2 指纹取像的几种技术和特点 .....	169
10.4.3 指纹识别系统中的软件和固件 .....	169
10.4.4 指纹识别技术的优缺点 .....	170
10.4.5 指纹识别技术的可靠性问题 .....	171
10.4.6 指纹识别技术的应用系统 .....	171
10.4.7 指纹识别技术的一些应用 .....	171
10.5 语音识别系统 .....	172
10.6 网膜图像识别系统 .....	172
10.7 识别过程 .....	173
10.7.1 引入阶段 .....	173
10.7.2 识别阶段 .....	173
10.7.3 折中方案 .....	173
10.8 身份识别技术的评估 .....	174
10.8.1 Mitre 评估研究 .....	174
10.8.2 语音识别 .....	175
10.8.3 签名识别 .....	175
10.8.4 指纹识别 .....	176
10.8.5 系统间的比较 .....	176
10.9 身份识别系统的选择 .....	177
10.10 访问控制 .....	177
10.10.1 访问控制概念与原理 .....	177

10.10.2 访问控制策略及控制机构 .....	178
10.10.3 访问控制措施 .....	179
10.10.4 信息流模型 .....	181
10.11 访问控制类产品 .....	182
思考题 .....	185
<b>第 11 章 信息隐藏技术 .....</b>	<b>186</b>
11.1 信息隐藏技术原理 .....	186
11.1.1 信息隐藏模型 .....	186
11.1.2 信息隐藏系统的特征 .....	187
11.1.3 信息隐藏技术的主要分支与应用 .....	188
11.2 数据隐写术 .....	189
11.2.1 替换系统 .....	189
11.2.2 变换域技术 .....	193
11.2.3 扩展频谱 .....	194
11.2.4 对隐写术的一些攻击 .....	195
11.3 数字水印 .....	196
11.3.1 数字水印模型与特点 .....	196
11.3.2 数字水印主要应用领域 .....	197
11.3.3 数字水印的一些分类 .....	198
11.3.4 数字水印算法 .....	198
11.3.5 数字水印攻击分析 .....	200
11.3.6 数字水印研究状况与展望 .....	201
思考题 .....	202
<b>第 12 章 计算机信息系统安全法律与规范 .....</b>	<b>203</b>
12.1 信息安全立法 .....	203
12.1.1 信息社会中的信息关系 .....	203
12.1.2 信息安全立法的基本作用 .....	204
12.2 国外信息安全立法概况 .....	205
12.2.1 国外计算机犯罪与安全立法的演进 .....	205
12.2.2 国外计算机安全立法概况 .....	205
12.3 我国计算机信息系统安全保护立法 .....	207
12.3.1 《中华人民共和国计算机信息系统保护条例》 .....	208
12.3.2 补充了计算机犯罪条款的新《刑法》 .....	212
思考题 .....	213

# 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 and 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。

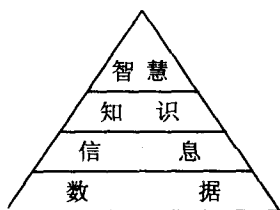


图 1-1 知识结构

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