21世纪高等教育计算机规划教材

COMPUTER

信息安全概论

Introduction to Information Security

张雪锋 主编

- 系统介绍当前广泛应用的信息安全技术
- 注重对主要知识内容的深入讨论
- 帮助读者建立信息安全意识的同时，使其“知其然，亦知其所以然”

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等教育计算机规划教材

信息安全概论

Introduction to Information Security

张雪锋 主编

人民邮电出版社
北京

图书在版编目（CIP）数据

信息安全概论 / 张雪锋主编. -- 北京 : 人民邮电出版社, 2014.3
21世纪高等教育计算机规划教材
ISBN 978-7-115-33282-0

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息安全－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2013)第317445号

内 容 提 要

本书系统地讲解了信息安全相关的基础知识，全书共有9章，介绍了信息安全领域的基本概念、基础理论和主要技术，并对信息安全管理和信息安全标准进行了简要介绍。主要内容包括信息技术与信息安全的基本概念、信息保密技术、信息认证技术、信息隐藏技术、操作系统与数据库安全、访问控制技术、网络安全技术、信息安全管理、信息安全标准与法律法规等。为了让读者能够及时检查学习的效果，把握学习的进度，每章后面都附有思考和练习题。

本书既可以作为信息安全、网络工程、计算机科学与技术、通信工程等本科专业学生信息安全基础课程的教材，也可供从事相关专业的教学、科研和工程技术人员参考。

◆ 主　　编　张雪锋
责任编辑　李海涛
责任印制　彭志环　焦志炜

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路11号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：787×1092　1/16
印张：14.75　　2014年3月第1版
字数：385千字　　2014年3月河北第1次印刷

定价：35.00元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前　言

随着信息技术的发展和普及，信息技术与人们的日常工作、学习和生活联系日益紧密，根据中国互联网络信息中心（CNNIC）2013 年 7 月发布的《中国互联网络发展状况统计报告（2013 年 7 月）》，截至 2013 年 6 月底，我国网民规模达 5.91 亿，互联网普及率为 44.1%，这些数据表明，中国网民的规模已经非常庞大。而该中心发布的《2012 年中国网民信息安全状况研究报告》表明，总体来看，目前中国网民只是简单地被灌输了要“重视信息安全”，但其实对其形成的原因认识并不清晰，形象地说，中国网民的信息安全意识处于“知其然，不知其所以然”的阶段，很多网民知道要重视信息安全，但并不知道为什么要重视，当然就更不知道如何解决自身面临的信息安全问题。因此，人们在享受着信息技术给自身工作、学习和生活带来便捷的同时，对信息的安全问题也日益关注。如何保障信息的安全存储、传输、使用，如何实现信息的保密性、完整性、可用性、不可否认性和可控性，成为困扰信息技术进一步发展的关键问题之一。当前，信息的安全问题不仅涉及人们的个人隐私安全，而且与国家的金融安全、政治安全、国防安全息息相关，大多数国家已经将信息安全上升到国家战略的高度进行规划和建设，这为信息安全技术的发展和信息安全类专业人才的培养提供了广阔的前景，也提出了迫切的发展需求，对信息安全从业者来说，这是前所未有的机遇，也面临着前所未有的挑战。

为了能为在校本科生学习信息安全提供内容较新、论述较系统的教材，也能为相关领域的科研人员提供一本内容充实，具有一定实用性的参考书，我们编写了《信息安全概论》这本教材。

本书是作者在长期从事信息安全领域科研和教学的基础上编写的，概括介绍了信息安全的基本概念、基本原理和主要技术，进一步介绍了信息安全管理和信息安全标准。内容以当前被广泛应用的信息安全技术为主进行了系统介绍，对其性能进行了相应的分析，既突出了广泛性，又注重对主要知识内容的深入讨论。本书主要面向信息安全、网络工程、计算机科学与技术、通信工程等本科专业的学生使用，计划课时为 32～48 学时。学习该课程的学生需要具备计算机和高等数学方面的知识，同时应该掌握基本的网络知识。通过对本课程的学习，学生可以掌握基本的信息安全理论、方法和技术，对信息安全技术具备一定的实际应用能力。

当然，解决信息系统面临的安全问题是一项复杂的系统性工程，相应的信息安全解决方案应该是一种综合解决方案，实践证明，任何试图将信息安全问题解决方案单一化的想法都是不切实际的，信息安全解决方案应该是一项系统工程，它不是多种安全技术的简单叠加使用，而应该从系统的角度去综合考虑。从这个角度来看，本书涉及的信息安全技术相互之间既有联系，又有区别，因此，读者在学习的过程中，应该从系统的角度去学习和理解不同技术相关内容之间的关联。

衷心感谢本书的主审，他提出的许多宝贵的意见和建议使我们受益匪浅。为了使本书既包含信息安全的基础知识，又能反映这些基础知识涉及的最新研究成果，本书在编写过程中参考了国内外许多同行的论文、著作，引用了其中的观点、数据与结论，在此一并表示谢忱。

由于编者水平有限，书中难免存在错误和不妥之处，恳切希望广大读者批评指正。

编　者

2013 年 11 月

目 录

第1章 绪论

本章概要介绍信息安全涉及的基本概念，包括信息的基本概念、特征、性质、功能和分类，信息技术的产生和内涵，信息安全涉及的基本概念、信息安全的目标和属性以及信息安全的基本原则，当前面临的主要安全威胁及实现信息安全的主要技术，同时重点介绍了信息安全管理的主要内容及基本原则。

本章的知识要点、重点和难点包括：信息的定义和性质、信息安全的属性、实现信息安全的基本原则和主要的信息安全技术。

1.1 概　　述

随着全球信息化的飞速发展，特别是计算机技术与通信技术相结合而诞生的计算机互联网的发展和广泛应用，打破了传统的时间和空间的限制，极大地改变了人们的工作方式和生活方式，促进了经济和社会的发展，提高了人们的工作水平和生活质量。

根据中国互联网络信息中心（CNNIC）2013 年 7 月发布的《中国互联网络发展状况统计报告（2013 年 7 月）》，截至 2013 年 6 月底，我国网民规模达 5.91 亿，较 2012 年底增加 2 656 万人，互联网普及率为 44.1%，较 2012 年年底提升了 2.0 个百分点，其中手机网民规模达 4.64 亿，较 2012 年年底增加 4 379 万人，网民中使用手机上网的人群占比提升至 78.5%。手机上网成为互联网发展的新动力：一方面，手机上网的发展推动了中国互联网的普及，尤其是为受网络、终端等限制而无法接入的人群和地区提供了使用互联网的可能性；另一方面，手机上网推动了互联网经济新的增长，基于移动互联网的创新热潮为传统互联网类业务提供了新的商业模式和发展空间，网络即时通信的网民规模迅速增加，电子商务类应用的使用率上升。

以上数据充分说明，信息技术已经与人们的日常生活、学习和工作息息相关。在信息化日益普及的今天，伴随着信息技术的广泛应用，当前，信息资源不仅成为人们日常生活、学习、工作中的基础资源，而且日益成为国家和社会发展的重要战略资源。国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全成为维护国家安全和社会稳定的一个焦点，各国都给予极大的关注和投入。

在我国，与信息技术被广泛应用形成鲜明对比的是信息安全问题日益突出，目前，我国已经成为信息安全事件的主要受害国之一。中国互联网络信息中心（CNNIC）2012 年 10 月发布的《2012 年中国网民信息安全状况研究报告》表明，虽然多年来我国不断加强信息安全的治理工作，但信息安全问题仍然十分严重，新的信息安全事件不断出现，且迅速向更多网民蔓延，导致信息安全事件的情境日

益复杂多样化，信息安全所引起的直接经济损失已达到很大规模，发起信息安全事件的因素已从此前的好奇心理升级为明显的逐利性，经济利益链条已然形成，信息安全事件中所涉及的信息类型、危害类型越来越多，且日益深入涉及网民的隐私，潜在的后果更严重。与此同时，我国的广大网民缺乏关于信息安全的知识，对信息安全的危害性并不清晰，采取的信息安全保护措施还未达到较好的水平，很多人并不具备处理信息安全事件的能力。

根据以上分析，信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题，它不但是发挥信息革命带来的高效率、高效益的有力保证，而且是抵御信息侵略的重要屏障。信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世界各国都在奋力攀登的制高点。从大的方面来说，信息安全问题已威胁到国家的政治、经济和国防等领域；从小的方面来说，信息安全问题已威胁到个人的隐私能否得到保障。因此，信息安全已成为社会稳定、安全的必要前提条件。信息安全问题全方位地影响我国的政治、军事、经济、文化、社会生活的各个方面，如果解决不好，将使国家处于信息战和高度经济金融风险的威胁之中。

信息安全不仅要保证信息的保密性、完整性，也就是关注信息自身的安全，防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的泄密或被非法使用等问题，而且还要保证信息的可用性、可控性，保证人们对信息资源的有效使用和管理。

1.2 信息与信息技术

在人类社会的早期，人们对信息的认识比较肤浅和模糊，对信息的含义没有明确的定义。到了20世纪中期以后，随着科学技术的发展，特别是信息科学技术的发展，对人类社会产生了深刻的影响，迫使人们开始探讨信息的准确含义。

信息论是20世纪40年代后期从长期通信实践中总结出来的一门学科，是专门研究信息的有效处理和可靠传输的一般规律的科学。信息是系统传输和处理的对象，它载荷于语言、文字、数据、图像、影视和信号等之中，要研究信息处理和传输的规律，首先要对信息进行定量的描述，即信息的度量，这是信息论研究的出发点。但要对通常含义下的信息（如知识、情报、消息等）给出一个统一的度量是困难的，因为它涉及客观和主观两个标准，而迄今为止最成功、应用最广泛的是建立在概率模型基础上的信息度量，进而建立在此种信息度量基础上的信息论成功地解决了信息处理和可靠传输中的一系列理论问题。

1.2.1 信息

1. 信息的定义

1928年，L.V. R. Hartley在*Bell System Technical Journal*上发表了一篇题为*Transmission of Information*的论文，在这篇论文中，他把信息理解为选择通信符号的方式，且用选择的自由度来计量这种信息的大小。Hartley认为，任何通信系统的发信端总有一个字母表（或符号表），发信者所发出的信息，就是他在通信符号表中选择符号的具体方式。假设这个符号表中一共有S个不同的符号，发送信息选定的符号序列包含N个符号，则从这个符号表中共有S^N种不同的选择方式，因而可以形成S^N个长度为N的序列。因此，就可以把发信者产生信息的过程看成是从S^N个不同的序列中选定一个特定序列的过程，或者说是排除其他序列的过程。

Hartley的这种理解在一定程度上解释了通信工程中的一些信息问题，但也存在一些严重的局

限性。主要表现在：一方面，他所定义的信息不涉及内容和价值，只考虑选择的方式，也没有考虑到信息的统计性质；另一方面，将信息理解为选择的方式，就必须有一个选择的主题作为限制条件。这些缺点使它的适用范围受到很大的限制。

1948 年，美国数学家 C. E. Shannon 在 *Bell System Technical Journal* 上发表了一篇题为 *A Mathematical Theory of Communication* 的论文，在对信息的认识方面取得了重大突破，堪称信息论的创始人。这篇论文以概率论为基础，深刻阐述了通信工程的一系列基本理论问题，给出了计算信源信息量和信道容量的方法和一般公式，得出了著名的编码三大定理，为现代通信技术的发展奠定了理论基础。

Shannon 指出，通信系统所处理的信息在本质上都是随机的，可以用统计方法进行处理。Shannon 在进行信息的定量计算的时候，明确地把信息量定义为随机不定性程度的减少，这就表明了他对信息的理解是：信息是用来减少随机不定性的东西。

虽然 Shannon 的信息概念比以往的认识有了巨大的进步，但仍存在局限性，这一概念同样没有包含信息的内容和价值，只考虑了随机型的不定性，没有从根本上回答“信息是什么”的问题。

1948 年，就在 Shannon 创立信息论的同时，N. Wiener 出版了专著 *Cybernetics: Control and communication in the animal and the machine*，创建了控制论，一门新的学科由此诞生。Wiener 从控制论的角度出发，认为“信息是人们在适应外部世界，并且这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容的名称”。Wiener 关于信息的定义包含了信息的内容与价值，从动态的角度揭示了信息的功能与范围，但也有局限性。由于人们在与外部世界的相互作用过程中，同时也存在着物质与能量的交换，Wiener 关于信息的定义没有将信息与物质、能量区别开来。

1975 年，意大利学者 G. Longo 在 *Information theory : new trends and open problems* 一书的序言中认为“信息是反映事物的形式、关系和差别的东西。它包含在事物的差异之中，而不在事物本身”。当然，“有差异就是信息”的观点是正确的，但是反过来说“没有差异就没有信息”就不够确切。所以，“信息就是差异”的定义也有其局限性。

据不完全统计，有关信息的定义有 100 多种，它们都从不同的侧面、不同的层次揭示了信息的特征与性质，但同时也都有这样或那样的局限性。

以下列出了几种典型的关于信息的定义。

（1）信息是指有新内容、新知识的消息——Hartley。

（2）信息是用来减少随机不定性的东西——Shannon。

（3）信息是人们在适应外部世界，并且这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容的名称——Wiener。

（4）信息是反映事物构成、关系和差别的东西，它包含在事物的差异之中，而不在事物的本身——Longo。

（5）信息是系统的组成部分，是物质和能量的形态、结构、属性和含义的表征，是人类认识客观的纽带。如物质表现为具有一定质量、体积、形状、颜色、温度、强度等性能。这些物质的属性都是以信息的形式表达的。我们通过信息认识物质、认识能量、认识系统、认识周围世界。

（6）信息是反应客观世界中各种事物特征和变化的知识，是数据加工的结果，信息是有用的数据。

（7）信息是经过加工后的数据，它对接收者有用，它对决策或行为有现实或潜在的价值。

（8）信息是指以声音、语言、文字、图像、动画、气味等方式所表示的实际内容。

为了进一步加深对信息概念的理解，下面讨论一些与信息概念关系特别密切、但又很容易混

淆的相关概念。

（1）信息与消息：消息是信息的外壳，信息则是消息的内核，也可以说，消息是信息的笼统概念，信息则是消息的精确概念。

（2）信息与信号：信号是信息的载体，信息则是信号所载荷的内容。

（3）信息与数据：数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。当然，在计算机里，所有的多媒体文件都是用数据表示的，计算机和网络上信息的传递都是以数据的形式进行，此时信息等同于数据。

（4）信息与情报：情报通常是指秘密的、专门的、新颖的一类信息，可以说所有的情报都是信息，但不能说所有的信息都是情报。

（5）信息与知识：知识是由信息抽象出来的产物，是一种具有普遍性和概括性的信息，是信息的一个特殊的子集，也就是说，知识就是信息，但并非所有的信息都是知识。

信息有许多独特的性质与功能，它是可以测度的，为了对其进行系统研究，形成了信息论的研究方向。

2. 信息的特征

信息有许多重要的特征，最基本的特征包括以下几点。

信息来源于物质，又不是物质本身；它从物质的运动中产生出来，又可以脱离源物质而寄生于媒体之中，相对独立地存在。信息是“事物运动的状态和状态变化方式”，但“事物运动的状态和状态变化方式”并不是物质本身，信息不等于物质。

信息也来源于精神世界。既然信息是事物运动的状态与状态变化方式，那么精神领域的事物运动（思维的过程）当然可以成为信息的一个来源。同客观物体所产生的信息一样，精神领域的信息也具有相对独立性，可以被记录并加以保存。

信息与能量息息相关，传输信息或处理信息总需要一定的能量来支持，而控制和利用能量需要信息来引导。但是信息与能量又有本质的区别，即信息是事物运动的状态和状态变化的方式，能量是事物做功的本领，提供的是动力。

信息是具体的并可以被人（生物、机器等）所感知、提取、识别，可以被传递、储存、变换、处理、显示、检索、复制和共享。

正是由于信息可以脱离源物质而载荷于媒体物质，可以被无限制地进行复制和传播，因此，信息可为众多用户所共享。

3. 信息的性质

信息具有下面一些重要的性质。

（1）普遍性：信息是事物运动的状态和状态变化的方式，因此，只要有事物的存在，只要事物在不断地运动，就会有它们运动的状态和状态变化的方式，也就存在着信息，所以信息是普遍存在的，即信息具有普遍性。

（2）无限性：在整个宇宙时空中，信息是无限的，即使是在有限的空间中，信息也是无限的。由于一切事物运动的状态和方式都是信息，而事物是无限多样的，事物的发展变化更是无限的，因而信息是无限的。

（3）相对性：对于同一个事物，不同的观察者所能获得的信息量可能不同。

（4）传递性：信息可以在时间上或在空间中从一点传递到另一点。

（5）变换性：信息是可变换的，它可以用不同载体以不同的方法来载荷。

（6）有序性：信息可以用来消除系统的不定性，增加系统的有序性。获得了信息，就可以消

除认识主体对于事物运动状态和状态变化方式的不定性。信息的这一性质对人类具有特别重要的价值。

（7）动态性：信息具有动态性质，一切信息都随时间而变化，因此，信息是有时效的。由于事物本身在不断发展变化，因而信息也会随之变化。脱离了母体的信息因为不再能够反映母体的新的运动状态和状态变化方式而使其效用降低，以至完全失去效用，这就是信息的时效性。所以人们在获得信息之后，不能就此满足，要不断补充和更新。

（8）转化性：在一定的条件下，信息可以转化为物质、能量。

上面的这些是信息的主要性质。了解信息的性质，一方面有助于对信息概念的进一步理解，另一方面也有助于人们更有效地掌握和利用信息。一旦信息被人们有效而正确地利用时，就可能在同样的条件下创造更多的物质财富和能量。

4. 信息的功能

信息的基本功能在于维持和强化世界的有序性，可以说，缺少物质的世界是空虚的世界，缺少能量的世界是死寂的世界，缺少信息的世界是混乱的世界。信息的社会功能则表现在维系社会的生存，促进人类文明的进步和人类自身的发展。

信息具有许多有用的功能，主要表现在以下几个方面。

（1）信息是一切生物进化的导向资源。生物生存于自然环境之中，而外部自然环境经常发生变化，如果生物不能得到这些变化的信息，生物就不能及时采取必要的措施来适应环境的变化，就可能被变化的环境所淘汰。

（2）信息是知识的来源。知识是人类长期实践的结晶，知识一方面是人们认识世界的结果，另一方面又是人们改造世界的方法，信息具有知识的秉性，可以通过一定的归纳算法被加工成知识。

（3）信息是决策的依据。决策就是选择，而选择意味着消除不确定性，意味着需要大量、准确、全面与及时的信息。

（4）信息是控制的灵魂。这是因为，控制是依据策略信息来干预和调节被控对象的运动状态和状态变化的方式。没有策略信息，控制系统便会不知所措。

（5）信息是思维的材料。思维的材料只能是“事物运动的状态和状态变化的方式”，而不可能是事物的本身。

（6）信息是管理的基础，是一切系统实现自组织的保证。

（7）信息是一种重要的社会资源。虽然人类社会在漫长的进化过程中一直没有离开信息，但是只有到了信息时代的今天，人类对信息资源的认识、开发和利用才可以达到高度发展的水平。现代社会将信息、材料和能源看成支撑社会发展的三大支柱，充分说明了信息在现代社会中的重要性。信息安全的任务是确保信息功能的正确实现。

5. 信息的分类

信息是一种十分复杂的研究对象，为了有效地描述信息，一定要对信息进行分类，分门别类地进行研究，由于目的和出发点的不同，信息的分类也不同。

从信息的性质出发，信息可以分为：语法信息、语义信息和语用信息。

从信息的过程出发，信息可以分为：实在信息、先验信息和实得信息。

从信息的地位出发，信息可以分为：客观信息和主观信息。

从信息的作用出发，信息可以分为：有用信息、无用信息和干扰信息。

从信息的逻辑意义出发，信息可以分为：真实信息、虚假信息和不定信息。

从信息的传递方向出发，信息可以分为：前馈信息和反馈信息。

从信息的生成领域出发，信息可以分为：宇宙信息、自然信息、社会信息和思维信息等。

从信息的应用部门出发，信息可以分为：工业信息、农业信息、军事信息、政治信息、科技信息、经济信息和管理信息等。

从信息源的性质出发，信息可以分为：语音信息、图像信息、文字信息、数据信息和计算信息等。

从信息的载体性质出发，信息可以分为：电子信息、光学信息和生物信息等。

从携带信息的信号形式出发，信息可以分为：连续信息、离散信息和半连续信息等。还可以有其他的分类原则和方法，这里不再赘述。

从上面的讨论可以看到描述信息的一般原则是：要抓住“事物运动的状态”和“状态变化的方式”这两个基本的环节来描述。事物运动的状态和状态变化的方式描述清楚了，信息也就描述清楚了。

1.2.2 信息技术

1. 信息技术的产生

任何一门科学技术的产生和发展都不是偶然的，而是源于人类社会实践活动的实际需要。“科学”是扩展人类各种器官功能的原理和规律，而“技术”则是扩展人类各种器官功能的具体方法和手段。从历史上看，在很长的一段时间里，人类为了维持生存而一直采用优先发展自身体力功能的战略，因此，材料科学与技术和能源科学与技术就相继发展起来。与此同时，人类的体力功能也日益加强。

虽然信息也很重要，但在生产力和生产社会化程度不高的时候，一方面，人们凭借自身的信息器官的能力，就足以基本上满足当时认识世界和改造世界的需要了；另一方面，从发展过程来说，在物质资源、能量资源、信息资源之间，相对而言，物质资源比较直观，信息资源比较抽象，而能量资源则介于两者之间。由于人类的认识过程必然是从简单到复杂，从直观到抽象，因而必然是材料科学与技术的发展在前，接着是能源科学与技术的发展，而后才是信息科学与技术的发展。

人类的一切活动都可以归结为认识世界和改造世界。从信息的观点来看，人类认识世界和改造世界的过程，就是一个不断从外部世界的客体中获取信息，并对这些信息进行变换、传递、存储、处理、比较、分析、识别、判断、提取和输出等，最终把大脑中产生的决策信息反作用于外部世界的过程。

这个生理的信息处理基本过程如图 1-1 所示。

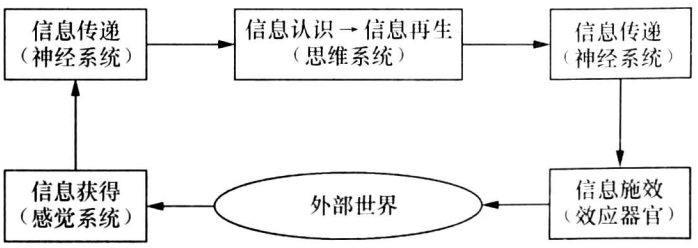

图 1-1　生理信息处理模型

但是，随着材料科学与技术、能源科学与技术的迅速发展，人们对客观世界的认识取得了长

足的进步，不断地向客观世界的深度和广度发展，这时，人类的信息器官功能已明显滞后于行为器官的功能了。例如，人类要“上天”、“入地”、“下海”、“探微”，但与生俱来的视力、听力、大脑存储信息的容量、处理信息的速度和精度，越来越不能满足人类认识世界和改造世界的实际需要，这时，人类迫切需要扩展和延长自己信息器官的功能。从 20 世纪 40 年代起，人类在信息的获取、传输、存储、处理和检索等方面的技术与手段，以及利用信息进行决策、控制、指挥、组织和协调等方面的原理与方法，都取得了突破性的进展，且是综合的。这些事实说明现代人类所利用的表征性资源是信息资源，表征性的科学技术是信息科学技术，表征性的工具是智能工具。

2. 信息技术的内涵

对于信息技术（Information Technology，IT），目前还没有一个准确而又通用的定义，估计有数十种之多。笼统地说：信息技术是能够延长或扩展人的信息能力的手段和方法。但在本节后面的讨论中，将信息技术的内涵限定在下面定义的范围内，即信息技术是指在计算机和通信技术支持下，用以获取、加工、存储、变换、显示和传输文字、数值、图像、视频、音频以及语音信息，并且包括提供设备和信息服务两大方面的方法与设备的总称。

信息技术中的信息处理基本过程如图 1-2 所示。

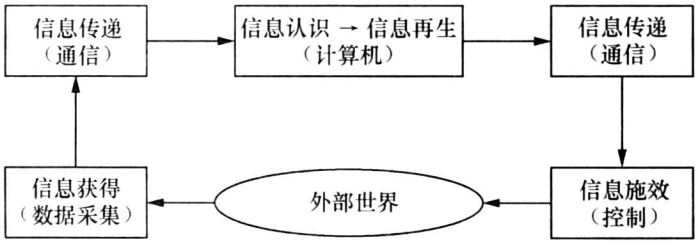

图 1-2　信息技术中的信息处理模型

由于在信息技术中信息的传递是通过现代的通信技术来完成的，信息处理是通过各种类型的计算机（智能工具）来完成的，而信息要为人类所利用，又必须是可以控制的。因此，也有人认为信息技术简单地说就是 3C：计算机（Computer）、通信（Communication）和控制（Control），即

$$IT = Computer + Communication + Control$$

以上的表述给出了信息技术的最主要的技术特征。

随着信息技术的迅速发展，随之而来的是信息在传递、储存和处理中的安全问题，而且安全问题越来越受到广泛的关注。

1.3　信息安全的内涵

1.3.1　基本概念

信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动了人类社会的发展和人类文明的进步，把人类带入了崭新的时代——信息时代。信息已成为社会发展的重要资源。然而，人们在享受信息资源所带来的巨大利益的同时，也面临着信息安全的严峻考验。信息安全已经成为世界性的问题。“安全”一词的基本含义为：“远离危险的状态或特性”，或

“主观上不存在威胁，主观上不存在恐惧”。安全是一个普遍存在的问题，安全存在于各种领域。随着计算机网络的迅速发展，人们对信息的存储、处理和传递过程中涉及的安全问题越来越关注，信息领域的安全问题变得非常突出。

国际标准化组织（ISO）对信息安全的定义是：“在技术上和管理上为数据处理系统建立的安全保护，保护计算机硬件、软件和数据不因偶然的和恶意的原因而遭到破坏、更改和泄露。”

信息安全是一个广泛和抽象的概念。所谓信息安全就是关注信息本身的安全，而不管是否应用了计算机作为信息处理的手段。信息安全的任务是保护信息财产，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等。这样可以使得我们在最大限度地利用信息的同时而不招致损失或使损失最小。

信息安全之所以引起人们的普遍关注，是由于信息安全问题目前已经涉及人们日常生活的各个方面。以网上交易为例，传统的商务运作模式经历了漫长的社会实践，在社会的意识、道德、素质、政策、法规和技术等各个方面都已经非常完善。然而对于电子商务来说，这一切却处于刚刚起步阶段，其发展和完善将是一个漫长的过程。假设你作为交易人，无论你从事何种形式的电子商务都必须清楚以下事实：你的交易方是谁？信息在传输过程中是否会被篡改（即信息的完整性）？信息在传送途中是否会被外人看到（即信息的保密性）？网上支付后，对方是否会不认账（即不可抵赖性）？如此等等。因此，无论是商家、银行还是个人，对电子交易安全的担忧是必然的，电子商务的安全问题已经成为阻碍电子商务发展的“瓶颈”之一，如何改进电子商务的安全现状，让用户不必为安全担心，是推动信息安全技术不断发展的动力。

信息安全可以说是一门既古老又年轻的学科，内涵极其丰富。信息安全不仅涉及计算机和网络本身的技术问题、管理问题，而且还涉及法律学、犯罪学、心理学、经济学、应用数学、计算机基础科学、计算机病毒学、密码学、审计学等学科。

信息安全经历了漫长的发展过程。从某种意义上说，从人类开始进行信息交流，就涉及了信息安全的问题。从古代的烽火传信到现在的网络通信，只要存在信息的交流，就存在信息的欺骗、破坏和窃取等安全威胁。从信息安全的发展过程来看，在计算机出现以前，通信安全以保密为主，密码学是信息安全的核心和基础，随着计算机的出现，计算机系统安全保密成为现代信息安全的重要内容，网络的出现使得大范围的信息系统的安全保密成为信息安全的主要内容。信息安全的宗旨是向合法的服务对象提供准确、正确、及时、可靠的信息服务；而对其他任何人员和组织，包括内部、外部乃至于敌对方，保持最大限度的信息的不透明性、不可获取性、不可接触性、不可干扰性、不可破坏性，而且不论信息所处的状态是静态的、动态的还是传输过程中的。

1. 信息的安全属性

信息安全研究所涉及的领域相当广泛。随着计算机网络的迅速发展，人们越来越依赖网络，人们对信息资产的使用更多的是通过计算机网络来实现的，在计算机和网络上信息的处理是以数据的形式进行，在这种情况下，信息就是数据。因而从这个角度来说，可以分为数据安全和系统安全，即信息安全可以从两个层次来看。

从消息的层次来看，信息安全的属性包括以下几个方面。

（1）完整性（Integrity）。完整性是指信息在存储或传输的过程中保持未经授权不能改变的特性，即对抗主动攻击，保证数据的一致性，防止数据被非法用户修改和破坏。对信息安全发动攻击的最终目的是破坏信息的完整性。

（2）保密性（Confidentiality）。保密性是指信息不被泄露给未经授权者的特性，即对抗被动攻击，以保证机密信息不会泄露给非法用户。

（3）不可否认性（Non-repudiation）。不可否认性也称为不可抵赖性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。发送方不能否认已发送的信息，接收方也不能否认已收到的信息。

从网络层次来看，信息安全的属性包括以下两个方面。

（1）可用性（Availability）。可用性是指信息可被授权者访问并按需求使用的特性，即保证合法用户对信息和资源的使用不会被不合理地拒绝。对可用性的攻击就是阻断信息的合理使用，例如破坏系统的正常运行就属于这种类型的攻击。

（2）可控性（Controllability）。可控性是指对信息的传播及内容具有控制能力的特性。授权机构可以随时控制信息的机密性，能够对信息实施安全监控。

要实现信息的安全，就是要通过技术手段和管理手段实现信息的上述 5 种安全属性。对于攻击者来说，就是要通过一切可能的方法和手段破坏信息的安全属性。

2. 信息安全的目标

基于以上分析，目前，实现信息安全的具体目标包括以下几个方面。

（1）真实性：能够实现对信息来源的判断确认，能够对伪造的信息进行鉴别。

（2）保密性：能够保证机密信息不被窃听，或窃听者不能了解信息的真实含义。

（3）完整性：能够保证数据的一致性，防止数据被非法用户篡改。

（4）可用性：能够保证合法用户对信息和资源的使用不会被不正当地拒绝。

（5）不可抵赖性：建立有效的责任机制，防止用户否认其行为。不可抵赖性对于电子商务尤为重要，是保证电子商务健康发展的基本保障。

（6）可控制性：对信息的传播及内容具有控制能力。

（7）可审查性：对出现的网络安全问题提供调查的依据和手段。

3. 信息安全的基本原则

为了达到信息安全的目标，各种信息安全技术的使用必须遵守以下 3 个基本原则：最小化原则、分权制衡原则和安全隔离原则。

最小化原则：受保护的敏感信息只能在一定范围内被共享，履行工作职责和职能的安全主体，在法律和相关安全策略允许的前提下，为满足工作需要，仅被授予其访问信息的适当权限，称为最小化原则。敏感信息的知情权一定要加以限制，是在“满足工作需要”前提下的一种限制性开放。

分权制衡原则：在信息系统中，对所有权限应该进行适当地划分，使每个授权主体只能拥有其中的一部分权限，使他们之间相互制约、相互监督，共同保证信息系统的安全。如果一个授权主体分配的权限过大，无人监督和制约，就隐含了“滥用权力”、“一言九鼎”的安全隐患。

安全隔离原则：隔离和控制是实现信息安全的基本方法，而隔离是进行控制的基础。信息安全的一个基本策略就是将信息的主体与客体分离，按照一定的安全策略，在可控和安全的前提下实施主体对客体的访问。

1.3.2　安全威胁

1. 基本概念

随着计算机网络的迅速发展，使得信息的交换和传播变得非常容易。由于信息在存储、共享和传输中，会被非法窃听、截取、篡改和破坏，从而导致不可估量的损失。特别是一些重要的部门，如银行系统、证券系统、商业系统、政府部门和军事系统，在公共通信网络中进行信息的存