全国计算机等级考试三级教程

——信息安全技术

（2015年版）

教育部考试中心

高等教育出版社

全国计算机等级考试三级教程

——信息安全技术

（2015年版）

Quanguo Jisuanji Dengji Kaoshi Sanji Jiaocheng

——Xinxi Anquan Jishu

教育部考试中心

主编　贾春福

参编　刘　昕　刘哲理　崔宝江　王春东

高等教育出版社·北京

内容提要

本书是依据教育部考试中心制订的《全国计算机等级考试三级信息安全技术考试大纲（2013年版）》编写的。主要内容包括：信息安全保障概论、信息安全基础技术与原理、系统安全、网络安全、应用安全、信息安全管理、信息安全标准与法规。

本书内容全面、系统，几乎涵盖了信息安全领域的所有知识，并注重知识之间的关联和衔接；同时本书面向信息安全工程与实践，介绍了信息安全最新技术及其发展趋势。

本书可作为参加计算机等级考试三级考试的复习用书，也可作为高等学校信息安全技术专业课程教材，还可作为社会读者学习参考。

图书在版编目(CIP)数据

全国计算机等级考试三级教程:2015年版.信息安全技术/教育部考试中心编.--北京:高等教育出版社,2014.11

ISBN 978-7-04-041382-3

Ⅰ.①全… Ⅱ.①教… Ⅲ.①电子计算机-水平考试-教材②信息安全-安全技术-水平考试-教材 Ⅳ.①TP3

中国版本图书馆CIP数据核字(2014)第249680号

策划编辑 何新权　　责任编辑 柳秀丽　　封面设计 杨立新　　版式设计 于 婕

责任校对 陈旭颖　　责任印制 韩 刚

出版发行 高等教育出版社
社　　址 北京市西城区德外大街4号
邮政编码 100120
印　　刷 保定市中画美凯印刷有限公司
开　　本 787mm×1092mm 1/16
印　　张 27.5
字　　数 680千字
购书热线 010-58581118

咨询电话 400-810-0598
网　　址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.landraco.com
http://www.landraco.com.cn
版　　次 2014年11月第1版
印　　次 2014年11月第1次印刷
定　　价 55.00元

物料号 41382-00

积极发展全国计算机等级考试 为培养计算机应用专门人才、促进信息产业发展作出贡献

（序）

中国科协副主席　中国系统仿真学会理事长
第五届全国计算机等级考试委员会主任委员
赵沁平

当今，人类正在步入一个以智力资源的占有和配置，知识生产、分配和使用为最重要因素的知识经济时代，也就是小平同志提出的“科学技术是第一生产力”的时代。世界各国的竞争已成为以经济为基础、以科技（特别是高科技）为先导的综合国力的竞争。在高科技中，信息科学技术是知识高度密集、学科高度综合、具有科学与技术融合特征的学科。它直接渗透到经济、文化和社会的各个领域，迅速改变着人们的工作、生活和社会的结构，是当代发展知识经济的支柱之一。

在信息科学技术中，计算机硬件及通信设施是载体，计算机软件是核心。软件是人类知识的固化，是知识经济的基本表征，软件已成为信息时代的新型“物理设施”。人类抽象的经验、知识正逐步由软件予以精确地体现。在信息时代，软件是信息化的核心，国民经济和国防建设、社会发展、人民生活都离不开软件，软件无处不在。软件产业是增长快速的朝阳产业，是具有高附加值、高投入高产出、无污染、低能耗的绿色产业。软件产业的发展将推动知识经济的进程，促进从注重量的增长向注重质的提高方向发展。软件产业是关系到国家经济安全和文化安全，体现国家综合实力，决定21世纪国际竞争地位的战略性产业。

为了适应知识经济发展的需要，大力促进信息产业的发展，需要在全民中普及计算机的基本知识，培养一批又一批能熟练运用计算机软件技术的各行各业的应用型人才。

1994年，国家教委（现教育部）推出了全国计算机等级考试，这是一种专门评价应试人员对计算机软硬件实际掌握能力的考试。它不限制报考人员的学历和年龄，从而为培养各行业计算机应用人才开辟了一条广阔的道路。

1994年是推出全国计算机等级考试的第一年，当年参加考试的有1万余人，2012年报考人数已达549万人。截至2013年年底，全国计算机等级考试共开考38次，考生人数累计达5 422万人，有2 067万人获得了各级计算机等级证书。

事实说明，鼓励社会各阶层人士通过各种途径掌握计算机应用技术，并通过等级考试对他们的能力予以科学、公正、权威性的认证，是一种比较好的、有效的计算机应用人才培养途径，符合我国的具体国情。等级考试同时也为用人部门录用和考核人员提供了一种测评手段。从有关公司对等级考试所作的社会抽样调查结果看，不论是管理人员还是应试人员，对该项考试的内容和

形式都给予了充分肯定。

计算机技术日新月异。全国计算机等级考试大纲顺应技术发展和社会需求的变化,从2010年开始对新版考试大纲进行调研和修订,在考试体系、考试内容、考试形式等方面都做了较大调整,希望等级考试更能反映当前计算机技术的应用实际,使培养计算机应用人才的工作更健康地向前发展。

全国计算机等级考试取得了良好的效果,这有赖于各有关单位专家在等级考试的大纲编写、试题设计、阅卷评分及效果分析等多项工作中付出的大量心血和辛勤劳动,他们为这项工作的开展作出了重要的贡献。我们在此向他们表示衷心的感谢!

我们相信,在21世纪知识经济和加快发展信息产业的形势下,在教育部考试中心的精心组织领导下,在全国各有关专家的大力配合下,全国计算机等级考试一定会以“激励引导成才,科学评价用才,服务社会选材”为目标,服务考生和社会,为我国培养计算机应用专门人才的事业作出更大的贡献。

前　言

本书是依据教育部考试中心制定的《全国计算机等级考试三级信息安全技术考试大纲(2013年版)》的内容组织编写的,系统地介绍了信息安全技术三级考试所涉及的相关内容和知识。全书共分7章。

第1章"信息安全保障概述":介绍了信息、信息技术和信息安全相关的知识,信息安全保障的内涵和意义,以及信息安全保障的总体思路和基本实践方法。

第2章"信息安全基础技术与原理":详细介绍了密码技术,包括对称密码与非对称密码、哈希函数、数字签名和密钥管理等内容;认证技术,包括消息认证和身份认证等知识;访问控制技术,包括访问控制模型和访问控制技术等内容;审计和监控技术,包括审计和监控的基本内容、审计和监控的主要技术等。

第3章"系统安全":主要介绍了操作系统安全,包括操作系统安全基础和操作系统安全实践等内容;数据库安全,包括数据库安全基础和数据库安全实践等知识。

第4章"网络安全":详细介绍了网络安全基础知识、网络安全威胁技术和网络安全防护技术,其中网络安全技术包括:防火墙、入侵检测系统与入侵防御系统、PKI、VPN和网络安全协议等内容。

第5章"应用安全":主要介绍了软件漏洞概念与原理、软件安全开发、软件安全检测、软件安全保护,以及恶意程序及其分析和Web应用系统安全等内容。

第6章"信息安全管理":详细介绍了信息安全管理体系、信息安全风险评估和信息安全管理措施等方面的内容。

第7章"信息安全标准与法规":主要介绍了信息安全标准、信息安全法律法规与国家政策,以及信息安全从业人员道德规范等方面的内容。

本书的特点主要表现为:内容全面系统,教程几乎涵盖了信息安全领域的所有知识内容和知识点,内容组织注意了知识之间的关联和衔接;注重基础知识和基本技能,面向信息安全工程与实践。通过学习每章所涉及的基本概念、基本原理、基本技术和基本方法,读者同时还能接触一些重要的信息安全实用技术,了解最新的技术及其发展趋势使读者能够很好地了解信息安全技术领域的最新的信息安全理念和技术。

本教程由中国石油大学(华东)刘昕(第1章)、南开大学刘哲理(第2章和第3章)、北京邮电大学崔宝江(第4章和第5章)、天津理工大学王春东(第6章和第7章)等编写,南开大学贾春福统稿。限于作者的水平和其他客观条件,书中难免有不妥或错误之处,望读者指正和提出宝贵意见。

编者

目　录

第1章　信息安全保障概述

导入语：本章概述了信息安全保障的相关内容。“信息安全保障背景”部分介绍了信息技术发展的各个阶段及其对社会产生的影响；“信息安全保障基础”部分讲述了信息安全发展阶段以及信息安全的含义、问题根源及其在社会中的地位和作用；“信息安全保障体系”部分讲解了信息安全保障基本体系框架，并详细阐述了典型的 P2DR 安全模型和 IATF 框架的基本原理；“信息安全保障基本实践”部分讲述了国内外实践概况和信息安全保障的基本工作内容。

考核目标：了解信息技术发展各个阶段的概况及其对社会、科技、人类生活所产生的影响；了解信息安全发展的各个阶段及其主要特征；理解信息安全的含义、问题根源及其在国家和信息社会中的地位和作用；理解信息安全保障体系；理解 P2DR 模型的基本原理及其数学表达公式的含义；理解 IATF 纵深防御思想及其对信息系统技术 4 个方面的安全需求划分；了解国内外信息安全保障工作概况；理解信息安全保障工作的各部分内容及其主要原则。

1.1　信息安全保障背景

1.1.1　信息技术及其发展阶段

人类社会的发展与进步是由社会生产力决定的。当今社会，科学技术作为第一生产力的作用日益凸显，信息技术作为现代先进科学技术体系中的前导要素，其所引发的社会信息化迅速地改变着社会的面貌，改变着人们的生产方式和生活方式，并对社会运行方式产生着巨大的影响。

那么，什么是“信息”呢？以往的关于信息的定义都从不同的侧面、不同的层次揭示了信息的特征和本质。美国数学家香农（Shannon）认为：通信系统所处理的信息本质上都是随机的，可以用统计的方法进行处理，在进行信息的定量计算时，明确地把信息量定义为随机不确定程度的减少。这表明了香农对信息的理解：信息是用于减少不确定性的东西。维纳（Wiener）认为：信息是人们在适应外部世界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。意大利学者朗高（Longo）认为：信息是反映事物的形式、关系和差异的东西，它包含在事物的差异中，而不在事物本身。我国信息论专家钟义信把信息定义为：事物运动的状态和状态变化的方式。

一般认为，钟义信的信息定义具有最大的普遍性，不仅涵盖所有其他信息定义，而且通过引入约束条件还能转化为所有其他信息的定义。为了加深对信息概念的理解，下面比较分析一下一些与信息相关且容易混淆的概念。

信息与消息：消息是信息的外壳，信息则是消息的内核；消息是信息的笼统概念，信息则是消

息的精确概念。

信息与信号:信号是信息的载体,信息则是信号所承载的内容。

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。

信息与情报:情报是指秘密的、专门的一类信息,所有的情报都是信息,但信息并不一定是情报。

信息与知识:知识是从信息中抽象出的产物,是一种具有普遍和概括性的信息,是信息的一个特殊子集。

关于"信息技术"的定义也很多。笼统地讲,信息技术是能够延伸或扩展人的信息能力的手段和方法。本书中信息技术是指,在计算机技术和通信技术的支持下,用于获取、传输、处理、存储、显示和应用文字、数值、图像、视频、音频等信息,并且包括提供设备和信息服务的方法和设备的总称。信息技术包括生产和应用两个方面。信息技术的生产主要体现在信息技术产业,包括计算机软硬件、电信设备、微电子生产等;信息技术的应用则体现在信息技术的扩散上,包括信息服务、管理信息系统等。在信息技术系统中,微电子技术、通信技术、计算机技术和网络技术可以称为信息技术的核心,它们的发展进程体现了信息技术的发展过程。

信息技术的产生与发展,大致经历了如下3个阶段。

第一阶段,电讯技术的发明。

信息技术的发展可以追溯到19世纪30年代电报电话的发明。1835年,莫尔斯(Morse)发明了电报。1837年,莫尔斯电磁式有线电报问世。1878年,人工电话交换局出现。1886年,马可尼发明了无线电报机。1876年,贝尔(Bell)发明了电话机。1892年,史瑞桥自动交换局设立。1912年美国Emerson公司制造出世界上第一台收音机。1925年,英国人约翰·贝德发明了世界上第一台电视机。

电讯技术的出现为信息技术的出现与发展奠定了基础。当今,微波通信、激光通信、电报、广播、电视、传真和卫星通信等相继问世,使信息开发利用趋向全球化、多样化、综合化。

第二阶段,计算机技术的发展。

1936年,英国数学家图灵(Turing)创造了图灵机理论。1937年,香农在美国麻省理工学院发表了《继电器和开关电路的符号分析》硕士论文,奠定了计算机二进制基础。世界上第一台现代电子计算机"埃尼阿克(ENIAC)"诞生于1946年2月14日的美国宾夕法尼亚大学。1945年,现代计算机之父冯·诺依曼等提出了"存储程序通用电子计算机方案"——EDVAC。现代计算机一直沿用着冯·诺依曼体系结构,可见其对计算机技术发展的影响。20世纪50年代末,第一代电子管计算机应用于军事科研过程的信息处理;60年代中期,第二代晶体管计算机向民用企业转移;60年代末,集成电路和大规模集成电路计算机接踵而至。

计算机技术的发展和应用,加快了人类奔向信息时代的步伐。

第三阶段,互联网的使用。

20世纪60年代末,美国出现了第一个用于军事目的的计算机网络ARPAnet。ARPAnet研究产生的一项非常重要的成果就是TCP/IP协议(Transmission Control Protocol/Internet Protocol),即传输控制协议/互联协议,使得连接到网络上的所有计算机能够相互交流信息。20世纪90年代,计算机网络发展成为全球性网络——因特网(Internet),计算机网络技术和网络应用得到了迅猛的发展。正是在这一阶段,才把电信、电话、电视、计算机、互联网络等连接起来(实现多媒

体传输)。

目前为止,几乎每个国家都与国际互联网有关联:从电子邮件到互联网的全部功能都得以开发利用。信息技术在这一阶段的飞速发展,深刻地影响着整个社会人们的工作和生活方式。

1.1.2 信息技术的影响

信息技术的飞速发展,对人类社会产生了重要影响,其主流是积极的,但也客观存在一些负面影响。

1. 信息技术的积极影响

(1) 对社会发展的影响

科学技术是第一生产力。如今信息技术已经成为科学技术前沿,人类社会正在从工业社会步入信息社会。随着信息技术的广泛应用,它已经引发了社会各个方面、各个层面和各个领域的深刻变革,加速了社会生产力的发展和人们生活质量的提高。信息资源继物质和能源之后将成为信息化社会最主要的支柱之一。信息技术的发展使得世界变成了一个地球村,如今人们可以及时分享社会进步带来的成果,减少地域差别和经济发展造成的差异。这样不仅促进了不同国家、不同民族之间的文化交流与学习,还使文化更加开放化和大众化。

(2) 对科技进步的影响

信息技术促进了新技术的变革,极大地推动了科学技术的发展。计算机技术的应用,帮助人们攻克了一个又一个科学难题,使得原本用人工需要花几十年甚至上百年才能解决的复杂计算,用计算机可能几分钟就能完成;应用计算机仿真技术可以模拟现实中可能出现的各种情况,便于验证各种科学假设。以微电子技术为核心的信息技术,带动了空间开发、新能源开发和生物工程等一批尖端技术的发展。此外,信息技术在基础学科中的应用及与其他学科的融合促进了新兴学科(如计算物理、计算化学等)和交叉学科(如人工智能、电子商务等)的产生和发展。

(3) 对人类生活的影响

信息技术的广泛应用,促进了人们工作效率和生活质量的提高以及工作方式和学习方式的转变。人们足不出户可知天下事,人不离家照样能办事。一部分人可以由原来的按时定点上班变为可以在家中上班,网上看病、网上授课、网上学习、网上会议、网上购物、网上洽谈生意、网上娱乐等正在成为一种新型的生活方式。网络技术、多媒体技术在教学上的应用,使得人们的学习方式更灵活,内容更丰富。

2. 信息技术的消极影响

对信息技术可能带来的一些负面影响,必须要有清醒和正确的认识。设法消除其不利影响具有重要意义。

(1) 信息泛滥

一方面是信息急剧增长,另一方面是人们消耗了大量的时间却找不到有用的信息。信息的增长速度超出了人们的承受能力,导致信息泛滥的出现。

(2) 信息污染

一些错误信息、虚假信息、污秽信息等混杂在各种信息资源中,使人们对错难分,真假难辨。人们如果不加分析,便容易上当受骗,受其毒害。

(3) 信息犯罪

随着信息技术应用的普及,人们对信息技术的依赖程度越来越高,信息安全已成为日益突出的问题。一些不法分子利用信息技术手段及信息系统本身的安全漏洞进行犯罪活动,如信息窃取、信息欺诈、信息攻击和破坏等,严重地危害着正常的社会秩序。

1.2 信息安全保障基础

在信息技术飞速发展的大背景下,人们的工作方式、生活方式和思想观念发生了巨大的改变,信息产业成为新的经济增长点。信息的获取、处理和安全保障能力已经成为一个国家综合国力的重要组成部分,信息安全事关社会稳定和国家安全。

1.2.1 信息安全发展阶段

信息安全的发展大致经历了3个主要阶段:通信保密阶段、计算机安全阶段和信息安全保障阶段。

1. 通信保密阶段

当代信息安全学起源于20世纪40年代的通信保密。这一时期,人们主要关注信息在通信过程中的安全性问题,即"机密性"。密码学是确保"机密性"的核心技术,这一时期密码学得到了快速的发展。

1949年,香农在发表的《保密系统的通信理论》论文中,首先用信息论的观点对信息保密问题作了全面的论述。这篇论文是现代通信安全的代表作,也是信息安全发展的重要里程碑。香农以概率统计的方法对消息源、密钥源、接收和截获的消息进行数学描述和分析,用不确定性来度量密码体制的保密性,阐明了密码系统、完善保密性、纯密码、理论保密性和实际保密性等重要概念,从而大大深化了人们对于信息保密和密码学的理解。这使得信息论成为研究密码学和密码分析学的一个重要理论基础,宣告了科学的密码学时代的到来。

2. 计算机安全阶段

20世纪60年代和70年代,计算机安全的概念开始逐步得到推行。1965年,美国率先提出了计算机安全(COMPUSEC)。随着多用户操作系统的出现,人们对信息安全的关注扩大为"机密性、访问控制与认证"。为了确保信息系统资产的机密性、完整性和可用性,安全操作系统设计技术得以被采用。

此时,计算机主要用于军方。1969年的Ware报告初步地提出了计算机安全及其评估问题。在研究方面,主要开展了Adept-50和Multics操作系统上的安全研究工作。

20世纪70年代是计算机安全的奠基时代。1972年,Anderson带领的小组完成了著名的Anderson报告。这个报告可以看做是计算机安全发展的里程碑,其中提出了计算机安全的主要问题以及相关的范型(如访问监控机)。在这一阶段,计算机主要的用途是军事和科研。访问控制关注信息的机密性,这一时期提出了强制访问控制策略和自主访问控制策略。其间进行的重要工作包括:1969年B. W. Lampson提出的访问控制矩阵,70年代Harrison、Ruzzo和Ullman提出的HRU模型,1976年David Bell和Leonard LaPadula提出的BLP模型,以及1977年Biba提出的BIBA模型。其中,BLP模型是影响深远的强制访问控制模型;BIBA模型是提出较早的面向完整性的访问控制模型;HRU模型给出了形式化的访问控制矩阵的描述,并提出了安全模型领域中

著名的 SAFTY 问题(授权传播的可判定性问题)。

在这一时期,密码学仍然得到了快速发展,最有影响的有两件大事件。第一件是 Diffie 和 Hellman 于 1976 年发表的论文《密码编码学新方向》,该文引发了密码学的一场革命。Diffie 和 Hellman 首次证明了在发送者和接收者之间无密钥交换的保密通信是可能的,从而开创了公钥密码学的新纪元。第二件是美国于 1977 年制定的数据加密标准 DES(Data Encryption Standard),它为加密算法的标准化奠定了基础。

20 世纪 80 年代的标志性特征之一是计算机安全的标准化工作。《可信计算机系统评估准则》(TCSEC,也称为橘皮书)是计算机系统安全评估的第一个正式标准,具有划时代的意义,为计算机安全评估奠定了基础。该准则于 1970 年由美国国防科学委员会提出,并于 1985 年 12 月由美国国防部公布。TCSEC 起初只是军用标准,后来发展至民用领域。TCSEC 将计算机系统的安全划分为 A、B(B1、B2、B3)、C(C1、C2)、D 共四个等级七个级别,等级由 A 到 D 依次降低。

在这之后,安全评估标准得到高度重视。世界各国根据自己的研究进展和实际情况,相继发布了一系列有关安全评估的准则和标准,如 TNI、TDI 等 TCSEC 解释性评估标准;英、法、德、荷等四国 20 世纪 90 年代初发布的信息技术安全评估准则(ITSEC);加拿大 1993 年发布的可信计算机产品评价准则(CTCPEC);美国 1993 年制定的信息技术安全联邦标准(FC);6 国 7 方,即加拿大、法国、德国、荷兰、英国、美国国家标准与技术研究院(NIST)及美国国家安全局(NSA),于 20 世纪 90 年代中期提出的信息技术安全性评估通用准则(CC:ISO 15408),简称通用准则,是评估信息技术产品和系统安全性的基础准则;我国于 2001 年 3 月正式颁布了 GB/T 18336:2001《信息技术安全技术信息技术安全性评估准则》(等同于 ISO/IEC 15408—1999)。

3. 信息安全保障阶段

20 世纪 90 年代以后,开始倡导信息保障(Information Assurance,IA)。

1995 年,在研究信息安全及网络战防御理论过程中,美国国防部提出了“信息安全保障体系”(IA)概念,并给出了“保护(Protection)—监测(Detection)—响应(Response)”三环节动态模型,即 PDR 模型。后来增加了恢复(Restore),变为 PDRR 模型。

为保护信息和系统资产,确保组织机构使命的顺利执行,需要综合技术、管理、过程、人员等方面的资源,以形成先进的技术和完善的管理协调机制,与之相关的有 BS 7799/ISO 17799 管理文件。

BS 7799 标准是由英国标准协会制定的信息安全管理标准,是国际上具有代表性的信息安全管理体系标准。该信息安全管理标准包括两个部分,即 BS 7799-1:1999《信息安全管理实施细则》和 BS 7799-2:1999《信息安全管理体系规范》。其中 BS 7799-1 标准已经正式转换为 ISO 国际标准,即 ISO 17799 信息安全管理体系实施指南。它综合了信息安全管理方面优秀的控制措施,可为各类组织和机构在信息安全方面提供建议性指南。

BS 7799/ISO 17799 主要章节包括范围、术语和定义、控制细则。BS 7799-2 还包括了信息安全管理体系要求,基本内容涉及信息安全政策、信息安全组织、信息资产分类与管理、个人信息安全、物理和环境安全、通信和操作安全管理、存取控制、信息系统的开放和维护、持续运营管理等。BS 7799-1 实施细则主要是给组织机构管理者提供了信息安全管理的实施惯例,为确定大、中、小型组织的信息系统通用控制范围、控制方法提供了参考标准。BS 7799-2 详细说明了建立、实施和维护信息安全管理体系的要求,规定了根据组织的需要应实施的安全控制要求,可以

作为第三方认证的标准。

1998 年 10 月,美国 NSA 颁布了信息保障技术框架(IATF)1.1 版。此后,NSA 于 1999 年 9 月和 2000 年 9 月分别颁布了 2.0 版和 3.0 版。本来 4.0 版应在 2001 年 9 月出台,可能受到 911 事件的影响,直到 2002 年 9 月,NSA 才颁布了 3.1 版。信息保障技术框架的研究和不断完善表明了美国军政各方对信息保障的认识逐步趋于一致。

我国专家在 1999 年提出了更为完善的"保护—预警(Warning)—监测—应急—恢复—反击(Counter-Attack)"即 PWDRRC 模型,使信息安全保障技术体系立于更为坚实的基础之上。

信息安全保障阶段关注"预警、保护、检测、响应、恢复、反击"整个过程,信息安全保障强调保护、检测、反应和恢复这四种能力,围绕人员、技术和管理这三个层面,以支持机构的任务和职能为目标,注重体系建设,强化组织与协调功能。

1.2.2 信息安全的含义

信息安全是一个广泛而抽象的概念。信息安全关注信息本身的安全,其任务是保护信息资产,防止偶然的或未经授权者对信息的恶意泄露、修改和破坏而导致信息的不可靠或无法处理等,使得在最大限度利用信息的同时不会导致损失或损失最小。从信息安全的发展历程可以看出,信息安全在不同的发展阶段具有不同的内涵。在不同信息应用领域,存在的安全问题也不同;所站的角度不同,对信息安全的理解也不尽相同。

目前,在网络信息时代,信息安全的内容已由机密性、完整性、可获性和规则性等数据安全与规约的安全概念,扩展到鉴别、授权、访问控制、抗抵赖性和可服务性,以及基于内容的个人隐私、知识产权等的系统保护安全内容。这些安全问题都要依靠密码技术、数字签名、身份认证、防火墙、安全审计、灾难恢复、防病毒、防黑客入侵等安全机制加以解决。

国际标准化组织(ISO)给出的信息安全定义为:为数据处理系统建立和采取的技术和管理的安全保护,保护计算机硬件、软件数据不因偶然或者恶意的原因而遭到破坏、更改和泄露。国内对信息安全的定义是指:信息网络的硬件、软件及其系统中的数据受到保护,不受偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续、可靠、正常地运行,信息服务不中断。

从信息网络系统看,现代信息安全主要包含两层含义:

一是运行系统的安全,包括严格而科学的管理,如对信息网络系统的组织管理、监督检查;规章制度的建立、落实与完善;管理人员的责任心、预见性、警惕性等;法律、政策的保护,如用户是否有合法权利,政策是否允许等;物理控制安全,如机房加锁、线路安全、环境适宜等;硬件运行安全;操作系统安全,如数据文件是否保护等;灾害、故障恢复;死锁的避免和解除;防止电磁信息泄露等。

二是系统信息的安全,包括用户口令鉴别;用户存取权限控制;数据存取权限、方式控制;审计跟踪;数据加密等。

信息安全的基本属性,主要包括以下 5 个方面:

① 完整性:是指信息在存储和传输过程中保持未经授权不能改变的特性,即保证数据的一致性,防止数据被非法用户篡改;

② 机密性:是指信息不被泄露给未经授权者的特性,即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 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正当地拒绝；

④ 可控制性：是指对信息的传播和内容具有控制能力的特性，即授权机构可以随时控制信息的机密性，能够对信息进行安全监控；

⑤ 不可否认性：也称不可抵赖性，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。发送方不能否认已经发送的信息，接收方也不能否认已经接收的信息。

信息安全的任务就是实现上述的5种安全属性，而攻击者则是想尽一切办法破坏上述信息安全属性。

整体上说，现代的信息安全是物理安全、网络安全、数据安全、信息内容安全、信息基础设施安全与公共、国家信息安全的总和，是多层次、多因素、多目标的复合系统。

1.2.3 信息系统面临的安全风险

随着信息网络系统的迅速发展和全面普及，人与计算机的关系发生了质的变化，人类社会与计算机和网络组成了一个巨大系统，出现了一个全新的世界——网络社会。人类对信息网络的依赖越来越强，不仅人们的政治经济文化生活依赖于网络，而且个人、企业、民族、国家乃至全人类的安全（包括金融安全、经济安全、政治安全、军事安全、科技安全、文化安全等）也建立在计算机和网络之上。因此，信息安全的内涵正在发生着前所未有的根本性变化。网络社会的信息安全不仅涉及个人权益、企业生存、金融风险防范、社会稳定和国家安全，而且关系到环境安全、生态安全和人类安全。

信息系统面临各种各样的安全风险，主要的安全威胁有：

① 信息泄露：信息被泄露或透露给非授权的实体。

② 破坏信息的完整性：在未授权的情况下数据被增删、修改或破坏而受到损失。

③ 拒绝服务：停止服务，阻止对信息或其他资源的合法访问。

④ 非授权访问：没有预先经过同意使用网络或计算机资源。

⑤ 授权侵犯：利用授权将权限用于其他非法目的，也称作“内部攻击”。

⑥ 业务流分析：通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

⑦ 窃听：借助于相关设备和技术手段窃取系统中的信息资源和敏感信息。例如，对通信线路中传输信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄漏截取有用信息等。

⑧ 物理侵入：侵入者绕过物理控制而获得对系统的访问。例如，旁路控制是指攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权，绕过防线守卫者侵入系统的内部。

⑨ 恶意代码：计算机病毒、木马、蠕虫等破坏计算机系统或窃取计算机中敏感数据的代码。

⑩ 假冒和欺诈：通过欺骗通信系统（或用户）使得非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户。

⑪ 抵赖：否认自己曾经发布过的消息，伪造对方来信等。

⑫ 重放攻击：又称重播攻击、回放攻击，是指基于非法的目的，攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的。重放攻击主要用于身份认证过程，破坏认证的正确性。

⑬ 陷阱门:通常是编程人员在设计系统时有意建立的进入手段。当程序运行时,在正确的时间按下正确的键,或提供正确的参数,就能绕过程序提供的正常安全检查和错误跟踪检查。

⑭ 媒体废弃:从废弃的磁碟或打印过的存储介质中获得敏感信息。

⑮ 人员不慎:授权的人为了各种利益或由于粗心,将信息泄露给非授权的人。

上述给出的是一些常见的安全威胁,这些威胁可以针对物理环境、通信链路、网络系统、操作系统、应用系统和管理系统等。

1.2.4 信息安全问题产生根源

信息系统的安全风险隐患来源于信息系统自身存在的脆弱性和信息系统面临的各种安全威胁。

(1) 信息安全内因:信息系统的复杂性

信息系统(Information System)是由人、计算机及其他外围设备等组成的,用于信息收集、传递、存储、加工、维护和使用的系统。信息系统本身是脆弱的,主要原因有:

① 组成网络的通信和信息系统的自身缺陷。现有的计算机系统存在许多安全问题,在客观上导致了计算机系统安全上的脆弱性。由于人类的认知能力和实践能力的局限性,在系统设计和开发过程中会产生各种各样的错误和遗漏,成为安全隐患。系统越庞大越复杂,安全隐患越多。1999 年,安全应急响应小组论坛(Forum of Incident Response and Security Teams,FIRST)的专家指出:每千行程序中至少有一个漏洞。随着系统的功能越来越强大,系统的复杂性不断增加,漏洞也就越来越多。

② 互联网的开放性。由于网络协议体系和实现是开放的,互联网缺少足够安全的设计,因此其中的漏洞会被熟悉协议的人利用。信息和数据在网络中是共享的,可以实现远程访问。信息系统的脆弱性使其容易受到来自系统外部的威胁,即信息系统运行环境存在着具有特定威胁动机的威胁源。这些威胁源会使用各种攻击手段,利用信息系统运行环境中的各种脆弱性,对信息系统造成相应的风险,由此产生信息安全事件和问题。

(2) 信息安全的外因:人为的和环境的威胁

① 人为原因。很多系统内部和外部的攻击者非法入侵、破坏系统和窃取信息。网络上存在的黑客网站使得获得攻击工具非常容易,黑客技术越来越易于掌握,导致网络面临的威胁越来越多、越来越大。

② 自然环境的原因。信息系统都是在一定的自然环境下运行的,自然灾害对信息系统的威胁是多方面的。地震、火灾、水灾、风灾等各种自然灾害都可能对信息系统造成毁灭性的破坏。

1.2.5 信息安全的地位和作用

在当今的信息时代和网络社会中,信息安全具有头等重要的地位,它是一切安全的重中之重,是社会发展的首要条件,是民族振兴的根本保障,是 21 世纪各国努力争夺的制高点。

(1) 信息安全是网络时代国家生存和民族振兴的根本保障

第一,信息安全是 21 世纪经济安全、国家安全和民族振兴的首要条件。在和平与发展成为时代主题的信息时代,网络及其应用是社会发展的基础。国家安全已不单纯是军事安全,而是越来越表现为经济安全和综合国力的强大,不发展就是最大的不安全。这就是说,国家安全与经济

安全越来越不可分割，而经济安全越来越依赖信息基础设施的安全，依靠信息资源的安全。因此，保证信息网络的安全性、可靠性，保证信息资源的安全性、可用性就成为头等重要的大事。如果不能保障网络安全和信息安全，就不可能获得信息化的效率和效益。在国际信息战威胁和国内外高技术犯罪的干扰破坏下，社会的经济生活就难以健康、有序地进行，国家的安全就无法保证，国家的生存就会受到威胁。因此，在21世纪，一个国家的信息安全保障能力不仅是其综合国力和经济实力的重要组成部分，而且是其国家安全的前提条件。

第二，信息安全是21世纪国家生存的前提条件。尽管人类刚刚步入信息时代，但是严峻的现实告诉我们，发展中国家普遍遭受到来自发达国家的信息霸权的威胁！众所周知，当代世界已经出现了三类国家：第一类是信息霸权国家，它们以先进的信息技术与网络技术作为手段，极力推行信息霸权主义，大搞电信霸权、软件技术霸权、信息利润霸权和网络霸权等；第二类是信息主权国家，它们有独立的信息主导权、独立的信息利润及防范信息霸权的手段；第三类是信息殖民地国家，它们被动地接受别国的信息，受到霸权国家的信息支配和剥削，没有防范信息霸权的能力。因此，信息技术和信息网络在国家和地区间的发展极不平衡，信息强国对于信息弱国已经形成了战略上的信息优势。居于信息劣势的国家的政治安全、经济安全、军事安全乃至民族文化传统，都将面临前所未有的冲击、挑战和威胁，互联网成为超级大国谋求跨世纪战略优势的新的工具。信息疆域不是以传统的地缘、领土、领空、领海来划分，而是以带有政治影响力的信息辐射空间来划分。信息疆域的大小和信息边界的安全关系到民族和国家在信息时代的兴衰存亡。在信息时代，一个缺乏信息安全保障能力的国家，是无法开拓自己的信息疆域的，也是无法保卫自己的信息边疆。这样的国家既无力构筑自己牢固的精神防线，更无力抢占并拥有经济生活和军事领域的自制信息权，它在信息社会中将是难以生存的。

（2）信息安全是信息社会健康发展和信息革命成功的关键因素

在信息社会，无论对于个人还是企业，民族还是国家，信息安全的重要性都是前所未有的。它既是行使和保障合法权益的基本手段，也是整个信息社会正常运行的先决条件。信息安全保障能力既是个人素质和企业实力的重要体现，也是国家主权和社会健康的重要标志。它不仅对个人、企业乃至国家的生存提出了新的挑战和要求，而且对国家的物质文明建设、精神文明建设、社会的有序管理、政权的安全巩固、国民素质的提高以及人类的全面自由发展等正发生着前所未有的深刻作用。在日益成为国家经济运行支柱的数字化、网络化环境中，如果没有信息安全，国家的经济体制与秩序安全、金融与货币安全、产业与市场安全、战略物资与能源安全、对外贸易与投资安全就不能得到有效保障，而保障社会生产和生活的正常秩序、保持社会各阶层的和睦共处、建立效率与公平兼顾的社会发展机制、控制犯罪、贫穷、腐败等消极现象、尊重多数人的权利与选择等社会和个人安全的要求在未来社会中也将难以实现。同样的，如果没有信息安全，作为信息社会之基础的信息网络、信息产业、信息基础设施和信息经济也将失控、紊乱、瘫痪甚至自毁。因此，从国家发展和社会运行的战略高度来看，信息安全既是人们畅游信息社会的“通行证”，也是信息革命成功的关键，是信息社会可持续发展的“守护神”。

（3）信息安全是网络时代人类生存和文明发展的基本条件

信息化使得人类社会出现了高度一体化的发展趋势，整个人类前所未有地结成一个利益共同体，一国的安全往往同时牵动他国的安全。因此，信息安全与网络安全已经不仅仅是某个国家、某个政府的事情，它日益成为人类整体的安全，成为人类文明的安全。从本质上说，信息是人