JISUANJIXINXIXITONGANQUANPEIXUNJIAOCHENG

计算机信息系统安全培训教程

公安部公共信息网络安全监察局 编

群众出版社

《计算机信息系统安全培训教程》

主　编：谢模乾
副主编：顾建国　袁旭阳　赵世强
撰稿人（以姓氏笔画为序）：
丁先存　丁建辉　王家玉　白　志
刘凤昌　赵世强　戴英侠
统稿人：刘凤昌　丁先存　徐志达　欧阳明

编者的话

互联网（Internet）的出现和迅猛发展，正在引发人类历史上又一场新的变革。计算机信息网络对国家社会政治、经济、文化运行的影响力和推动作用越来越大。网络改变了人们的工作、学习和生活方式，使信息的获取、传递、处理和利用更加便捷。然而，由于计算机信息网络的迅速发展和技术、管理等多方面的原因，使信息安全存在着极大的风险和隐患。

构筑我国的计算机信息网络安全体系是一项跨世纪的战略任务，加强对网络工作者和网络用户的安全意识教育是实施这一战略目标的基础。在公安部和人事部联合发出通知开展了三年计算机安全员培训工作的基础上，结合目前计算机信息网络安全保护理论和技术的最新发展，我们对原计算机安全员培训教材进行了较大的修改，重新出版，作为全国计算机安全员培训的统一教材。

全套教材分为两册：《计算机信息系统安全培训教程》和《计算机信息系统安全培训教程习题及相关法规》。

《计算机信息系统安全培训教程》撰稿人（以姓氏笔画为序）：丁先存、丁建辉、王家玉、白志、刘凤昌、赵世强、戴英侠。初稿经刘凤昌、丁先存、徐志达、欧阳明统稿后，由正、副主编审核定稿。

《计算机信息系统安全培训教程习题及相关法规》撰稿人（以姓氏笔画为序）：丁先存、丁建辉、王宏勇、王家玉、王景红、白志、刘凤昌、赵世强、戴英侠。初稿经刘凤昌、王宏勇、王景红统稿后，由正、副主编审核定稿。

《计算机信息系统安全培训教程》在编写的过程中，广泛吸纳了各方面的意见和建议，参考了有关的资料和教材。李文燕、马民虎、吴亚菲、崔书昆等同志对初稿提出了宝贵的修改意见，在此表示衷心感谢。安徽省公安厅孙建新副厅长、公共信息网络安全监察处田扬畅处长对教程编写工作给予关心和支持，对教程内容提出中肯的意见和建议，在此也一并表示感谢。

《计算机信息系统安全培训教程习题及相关法规》在编写过程中，习题部分主要采纳了1999年警官教育出版社编写的《计算机信息系统安全培训

习题集》的内容，对该书的全体参编人员深表谢意。

由于计算机信息系统安全保护理论和技术发展很快，计算机信息系统安全保护的法律法规，也正处于逐步完善的阶段。在本套教材编撰的过程中，难免有疏漏之处，欢迎广大读者批评指正，以便再版时修改。

编写组

2001 年 6 月 11 日

目 录

第一章 概 论

信息领域是当今最充满活力的领域，经济、贸易区域化、全球化使社会信息量急剧增加。信息将成为支撑国家政治、经济、军事、科技的重要战略资源和力量基础。自20世纪40年代计算机在美国诞生以来，计算机应用已逐渐普及社会的各个领域。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信息系统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”。一旦计算机系统受到攻击，不能正常工作，甚至全部瘫痪时，就会使整个社会陷入危机。尤其因特网（INTERNET）应用发展以来，它已不仅仅是我们工作和生活中不可缺少的工具，事实上它已经成为社会资源重组的根本工具，逐步渗透到社会的任何一个行业、任何一个部门，它已经涉及到国家安全与主权的重大问题。

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。安全法规的贯彻和安全技术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。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，水涨船高，安全是相对，没有一劳永逸的安全防范措施，计算机信息系统安全保护工作必须常抓不懈，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的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领域；信息与信息系统的安全管理，亦已成为社会公共安全工作的重要组成部分。

第一节 计算机信息系统及安全

为了深刻理解本书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。

一、计算机信息系统

现代（电子）信息系统大体上分为三类：

① 计算机信息系统。

② 广播电视系统。

③ 电信系统（程控电话、移动通信、无线通信等等），其中所谓计算机信息系统是

指“由计算机及其相关的和配套的设备、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”。其基本组成是：计算机实体、信息和人。

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。网络技术的应用，使得在空间、时间上原先分散、单立的信息，形成为庞大的信息资源系统。网络资源的共享，无可估量地提高了信息系统中信息的有效使用价值。

二、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、运行安全和人员安全等几个部分。人的安全主要是指计算机使用人员的安全意识、法律意识、安全技能等。下面就实体安全、信息安全和运行安全的内容做简单的说明。

（一）实体安全（或称物理安全）

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、雷电、噪声、外界电磁干扰、电磁信息泄漏、有害气体和其他环境事故（如电磁污染等）破坏的措施、过程。实体安全包括环境安全、设备安全和媒体安全三个方面。

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漏和破坏。因此，对计算机信息系统实体的保护是防止对信息威胁和攻击的首要一步，也是防止对信息威胁和攻击的屏障。

（二）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、应急四个方面的内容。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，其目标是保证系统能连续、正常地运行。

（三）信息安全

所谓计算机信息系统的信息安全是指防止信息资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辨识、控制，确保信息的保密性、完整性、可用性、可控性。针对计算机信息系统中信息存在形式和运行特点，则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、加密与鉴别七个方面。

三、计算机信息网络安全

（一）计算机信息系统安全和计算机信息网络安全的演变

计算机信息系统的安全问题始于20世纪60年代末期。当时，计算机信息系统的脆弱性问题逐渐暴露出来，引发了一些安全问题，被西方发达国家的政府和一些私营机构所识，开始了对计算机信息系统安全问题的研究。由于当时计算机的运行速度和性能比较落后，使用的范围也不广，将计算机信息系统安全问题作为核心机密严格加以控制，因此，对计算机信息系统的安全研究限制在比较小的范围以内。在六七十年代，人们把信息安全理解为是对信息的保密性、完整性和可用性的保护，这是主机计算机年代形成

的静态管理模式。

进入80年代，由于计算机本身强大的独立处理能力，计算机应用渗透到各个领域，个人电脑的发展非常迅速，就在90年代中期，PC机的发展，超过了网络的发展速度。到今天人们一连接上信息网络，才猛然发现计算机只有同网络相连，才是真正的计算机，在信息网络上，你已经不是在使用你自己的计算机，而是在使用一台资源浩瀚、地域辽阔、传递神速的庞大计算机。有了计算机，才有了信息网络，而信息网络又当仁不让的成为计算机的主体，计算机将会像电话机和电视机一样，仅仅是一台终端处理机。“计算机信息系统”的安全就演变成为“信息网络”的安全。

（二）静态安全和动态安全

每个用户都可以连接、使用乃至控制分布在世界上各个角落的联网计算机，因此计算机信息网络的安全内容更注重全网的动态安全，强调面向连接、面向用户的安全。从系统工程的角度，要求计算机信息网络具有可用性、完整性和保密性，现在又增加了具有动态内容的真实性（不可抵赖性）、可靠性和可控性，并给计算机信息网络可用性、完整性和保密性赋予新的动态内容。

1. 可用性

可用性即保证信息和计算机信息网络随时为授权者提供服务，而不要出现非授权者滥用却对授权者拒绝服务的情况，即使是计算机信息网络部分受损而需要降级使用时，仍能为授权者提供有效服务的性能。信息网络最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的。可用性的度量用信息网络正常使用时间和整个工作时间之比来度量。

可用性还应该满足信息网络以下要求：身份识别与确认；访问控制（包括自主访问控制和强制访问控制）；业务流控制（防止业务流量过度集中而引起网络阻塞）；路由选择控制（选择那些稳定可靠的子网、中断线或链路等）；审计跟踪。审计跟踪是把网络信息系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。审计跟踪的信息主要包括：被管客体等级，事件类型、事件时间、事件信息、事件回答以及事件统计等方面的信息。

2. 完整性

完整性即保证信息从真实的发信者传送到真实的收信者手中，传送过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的性能。影响网络信息完整性的主要因素有：设备故障、误码、人为攻击、计算机病毒、信息战攻击等。

保障网络信息完整性的主要方法有：

协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。

纠措编码方法：由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法。

密码校验和方法：它是抗篡改和传输失败的重要手段。

数字签名：保障信息不可否认。

公证：请求网络管理或中介机构进行证实，保障信息准确可信。

3. 保密性

保密性即保证信息为授权者享用而不泄漏给未经授权者。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

常用的保密技术包括：防侦收（使对方侦收不到有用的信息），防辐射（防止有用信息以各种途径辐射出去），信息加密（在密钥的控制下，用加密算法对信息进行加密处理），物理保密（利用各种物理方法保护信息不被泄露）。

保密性与完整性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。

4. 真实性（不可抵赖性）

真实性（不可抵赖性）也称作不可否认性。即保证信息的行为人要为自己的信息行为负责，在信息网络的信息交互过程中，确信参与者的真实同一性，所有参与者都不能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发言方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。信息网络要能够真实地提供保证社会依法管理所需要的公证、仲裁证据。

5. 可靠性

可靠性即保证信息系统不停顿地提供正常服务，使信息网络系统具备在规定条件下和规定的时间内完成规定的功能的性能。可靠性是系统安全的最基本要求之一，是所有信息网络的建设和运行目标。可靠性可以用公式描述为 R = MTBF/（MTBF + MTTR），其中 R 表示可靠性，MTBF 表示平均故障间隔时间，MTTR 表示平均故障修复时间。因此，增大可靠性的有效思路是增大平均故障间隔时间或者减少平均故障修复时间。增大可靠性的具体措施包括：提高设备质量、严格质量管理、配备必要的冗余和备份、采用容错、纠错和自愈等措施、选择合理的拓扑结构和路由分配、强化灾害恢复机制、分散配置和负荷等。

计算机信息网络的可靠性测度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，系统是否仍然能够提供一定程度的服务。增强抗毁性可以有效地避免因各种灾害（战争、地震等）造成的大面积瘫痪事件。

生存性是在随机破坏下系统的可靠性。生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响。这里，随机性破坏是指系统部件因为自然老化等造成的自然失效。

有效性是一种基于业务性能的可靠性。有效性主要反映在网络信息系统的部件失效情况下，满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内，程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、

培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

6. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。出于国家和机构的利益和社会管理的需要，保证管理者能够对信息实施必要的控制管理，以对抗社会犯罪和外敌侵犯。

第二节 计算机信息系统面临的威胁及其脆弱性

由于计算机信息系统已经成为信息社会另一种形式的“金库”和“保密室”，成为一些人窥视的目标；再者，由于计算机信息系统自身所固有的脆弱性，使计算机信息系统面临威胁和攻击的考验。

一、计算机信息系统受到的威胁

计算机信息系统的安全威胁同时来自内、外两个方面。

（一）外部威胁

1. 自然灾害

计算机信息系统仅仅是一个智能的机器，易受火灾、水灾、风暴、地震等破坏以及环境（温度、湿度、振动、冲击、污染）的影响。目前，我们不少计算机房并没有防震、防火、防水、避雷、防电磁泄漏或干扰等措施，接地系统地疏于周到考虑，抵御自然灾害和意义事故的能力较差。日常工作中因断电使设备损坏、数据丢失的现象时有发生。

2. 黑客的威胁和攻击

计算机信息网络上的黑客攻击事件越演越烈，已经成为具有一定经济条件和技术专长的形形色色攻击者活动的舞台。黑客破坏了信息网络的正常使用状态，造成可怕的系统破坏和巨大的经济损失。

3. 计算机病毒

计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一级计算机指令或者程序代码。

“计算机病毒”这个称呼十分形象，它像个灰色的幽灵无处不存、无时不在。它将自己附在其他程序上，在这些程序运行时进入到系统中扩散。一台计算机感染上病毒后，轻则系统工作效率下降，部分文件丢失，重则造成系统死机或毁坏，全部数据丢失。1999 年 4 月 26 日 CIH 病毒在全球造成的危害，足以显露计算机病毒的可怕。

据一份市场调查报告表明，我国约有 90% 的网络用户曾遭到过病毒的侵袭，并且其中大部分因此受到损失。病毒危害的泛滥，揭示了计算机系统本身和人们的意识在安全方面的薄弱。

4. 垃圾邮件和黄毒泛滥

一些人利用电子邮件地址的“公开性”和系统的“可广播性”进行商业、宗教、政治等活动，把自己的电子邮件强行“推入”别人的电子邮箱，甚至塞满人家的电子邮箱，强迫人家接受他们的垃圾邮件。

国际互联网络的广域性和自身的多媒体功能，也给黄毒的泛监提供了可乘之机。

5. 经济和商业间谍

通过信息网络获取经济和商业情报和信息的威胁大大增加。大量的国家和社团组织上网，丰富了网上的内容的同时，也为外国情报收集者提供了捷径，通过访问公告牌、网页以及内部电子邮箱，利用信息网络的高速信息处理能力，进行信息相关分析获取情报。

6. 电子商务和电子支付的安全隐患

计算机信息网络的电子商务和电子支付的应用，给我们展现了一幅美好的前景，但由于网上安全措施和手段的缺乏，阻碍了其快速的发展。一定要将“信息高速路”上的“运钞车”打造结实，将“电子银行”的“警卫”配备齐全，再开始运营。

7. 信息战的严重威胁

所谓信息战，就是为了国家的军事战略而采取行动，取得信息优势，干扰敌方的信息和信息系统，同时保卫自己的信息和信息系统。这种对抗形式的目标，不是集中打击敌方的人员或战斗技术装备，而是集中打击敌方的计算机信息系统，使其神经中枢似的指挥系统瘫痪。

信息技术从根本上改变了进行战争的方法，信息武器已经成为了继原子武器、生物武器、化学武器之后的第四类战略武器。

在海湾战争中，信息武器首次进入实战。伊拉克的指挥系统吃尽了美国的大亏：仅仅是在购买的智能打印机中，被塞进一片带有病毒的集成电路芯片，加上其他的因素，最终导致系统崩溃，指挥失灵，几十万伊军被几万联合国维和部分俘虏。美国的维和部队还利用国际卫星组织的全球计算机网络，为其建立军事目的的全球数据电视系统服务。

所以，未来国与国之间的对抗首先将是信息技术的较量。网络信息安全，应该成为国家安全的前提。

8. 计算机犯罪

计算机犯罪是利用暴力和非暴力形式，故意泄漏或破坏系统中的机密信息，以及危害系统实体和信息安全的不法行为。《中华人民共和国刑法》对计算机犯罪作了明确定义，即利用计算机技术知识进行犯罪活动并将计算机信息系统作为犯罪对象。

利用计算机犯罪的人，通常利用窃取口令等手段。非法侵入计算机信息系统，利用计算机传播反动和色情等有害信息，或实施贪污、盗窃、诈骗和金融犯罪等活动，甚至恶意破坏计算机系统。

（二）内部威胁

由于计算机信息网络是一个“人机系统”，所以内部威胁主要来自使用的信息网络系统的脆弱性和使用该系统的人。外部的各种威胁因素和形形色色的进攻手段之所以起作用，是由于计算机系统本身存在着脆弱性，抵御攻击的能力很弱，自身的一些缺陷常

常容易被非授权用户不断利用，外因通过内因起变化。

1. 软件工程的复杂性和多样性，使得软件产品不可避免地存在各种漏洞。世界上没有一家软件公司能够做到其开发的产品设计完全正确没有缺陷，而且永远也不可能做到。这些缺陷正是计算机病毒蔓延和黑客“随心所欲”的温床。

2. 存储器的容量非常大。一个硬盘甚至一张软盘足以存入一个单位或组织的保密信息，因此，被窃或丢失一张软盘造成的损失，可能造成大量国家、单位机密或敏感信息被窃。利用磁介质的剩磁效应，从一张已经被认为损坏的软盘中也可能恢复得到足够多的有用信息。

3. 电子数据的非物质特性。这使得不易发现它们是否被访问或修改过，磁盘上的文件被访问本身不会留下任何痕迹，你自己访问了某个文件与别人访问了这个文件后，不会有任何不同的特征在文件本身体现出来。

4. 电磁辐射也可能泄漏有用信息。已有试验表明，在一定的距离以内接收计算机因地线、电源线、信号线或计算机终端辐射导致的电磁泄漏产生的电磁信号，经过处理可复原正在处理的机密或敏感信息。

5. 网络环境下电子数据的可访问性对信息的潜在威胁比对传统信息的潜在威胁大得多。非网络环境下，任何一个想要窃密的人都必须先解决潜入秘密区域的难题。而在网络环境下，这个难题已不复存在，只要你有足够的技术能力和耐心。

6. 不安全的网络通信信道和通信协议。信息网络自身的运行机制是一种开放性的协议机制。网络结点之间的通信是按照固定的机制，通过交换协议数据单元来完成的，以保证信息流按“包”或“帧”的形式无差错地传输。那么，只要所传的信息格式符合协议所规定的协议数据单元格式，那么，这些信息“包”或“帧”就可在网上自由通行。至于这些协议数据单元是否来自源发方，其内容是否真实，显然无法保证。这是在早期制定协议时，只考虑信息的无差错传输所带来的固有的安全漏洞，更何况某些协议本身在具体的实现过程中也可能会产生一些安全方面的缺陷。对一般的通信线路，可以利用搭线窃听技术来截获线路上传输的数据包，甚至重放（一种攻击方法）以前的数据包或篡改截获的数据包后再发出（主动攻击），这种搭线窃听并不比用窃听器偷听别人的电话困难多少。对于卫星通信信道而言，则既需要有专门的接收设备（类似于电视信号的地面接收器），对设备的安装又要有较高的技术要求（如天线方位和角度的调整），以及其他参数的设置等。

7. 内部人员的不忠诚、人员的非授权操作和内外勾结作案是威胁计算机信息网络安全的重要因素，“没有家贼，引不来外鬼”就是这个道理。他们或因利欲熏心，或因对领导不满，或出于某种政治、经济或军事的特殊使命，从机构内部利用权限或超越权限进行违反法纪的活动。统计表明，信息网络安全事件中 60% ~ 70% 起源于内部。我们要牢记：“防内重于防外。”

二、计算机信息网络脆弱性引发的信息社会脆弱性和安全问题

计算机信息网络首先要网络化，网络是信息资源得以利用的基础，并将成为人们获取信息的基本手段；同时人们对网络的依赖给国民经济和国家安全也带来了巨大隐患。网络和信息时代给我们带来技术进步和生活便利的同时，也给国民经济和国家安全带来

了巨大隐患。信息网络受攻击，形成对信息社会的攻击；信息网络的脆弱性，引发了信息社会的脆弱性。

（一）技术被动性、依赖性引发的脆弱性

以网络方式获得和交流信息，已成为现代信息社会的重要特征。当网络的信息资源成为许多国家和许多用户的生命线时，一旦信息网络遭到入侵和破坏，其后果所带来的危害往往是社会性的、灾难性的。

（二）引发的国家安全问题

网络世界实际是一个电子化的社会，是对现实社会的映象。文化的自由主义、意识形态的多元化，使得网上的信息五色俱全；有真，有假；有利，有弊。同时，“网络社会”也存在“边界”——信息边界。“信息疆域”不是以传统的地缘、领土、领空、领海、领天来划分的，而是国家和政治团体传播力和影响力所能达到的无形空间。因而，同样存在着复杂的政治斗争、军事对抗和激烈的商业竞争。“信息疆域”的疆界、“信息边界”的安全，已经涉及到国家安全与主权的重大问题，关系到一个民族、一个国家在信息时代的兴亡。

为缩小与世界先进水平的差距，我国引进了不少外国设备：芯片基本依赖于进口，甚至网络产品都是来自国外。由于大部分引进设备都不转知识产权，我们很难获得完整的技术资料档案。这为今后扩展、升级和维护带来极大的麻烦。更可怕的是有些引进设备可能在出厂时，就隐藏了恶意的“定时炸弹”、“陷井”（某些操作系统为了安装其他公司的软件包而保留的一种特殊的管理程序功能）、计算机病毒。美国出口中国的密钥芯片上就为政府留了一个接口，供美国政府随时启动。甚至有一天忽然发现，网络黑客攻击或病毒程序恰恰就是来自于卖给我们产品的国家和地区。在非和平时期，这些预设的“机关”有可能对我们的信息网络安全与保密将构成致命的打击。

（三）引发的民族文化问题

互联网是在美国发展起来的，网上信息绝大多数是美国文化背景下的英文信息。不懂英文的人看不懂，懂英文的人接受的又是充满美国文化的传统和宣传，这实际上是一种文化殖民主义。它将冲淡和腐蚀以民族文化维系的世界各国多民族国家的民族传统，使其他国家的文化生存处于十分危险的境界。此外，境内外敌对势力和非法组织利用互联网进行煽动、渗透、组织、联络等非法活动进行反动宣传，煽动反政府情绪；利用互联网进行组党结社，公开吸纳成员，进行宗教渗透等各种分裂祖国、泄露国家秘密活动；利用互联网制作、复制、查阅、传播有害信息，宣扬封建迷信、邪教、色情、赌博、暴力、诬陷、诽谤他人等危害社会稳定的行为，这些行为不仅对社会主义精神文明造成破坏，并且必将危害社会公共安全。

第三节 计算机信息系统安全保护和监察

《中华人民共和国计算机信息系统安全保护条例》第三条，规范了计算机信息系统

安全保护的概念："计算机信息系统的安全保护，是指保障计算机及其相关的设备、设施（含网络）的安全、运行环境的安全，保障信息的安全，保障计算机功能正常发挥，以维护计算机信息系统的安全运行。"

一、计算机信息系统安全保护

（一）计算机信息系统安全保护的基本概念

计算机信息系统安全保护主要包括两个方面的内容，一是国家实施的安全监督管理，二是计算机信息系统使用单位自身的保护措施。实施计算机信息系统安全保护的措施包括：安全法规、安全管理、安全技术三个方面。

1. 安全法规

依法实施计算机信息系统安全保护是我们的一项基本原则。这里讲的安全法规应该包括法规、政策和技术规范三个层次。要使计算机信息系统安全运行，信息安全传递，需要靠必要的法律建设，以法制来强化计算机信息系统安全。这主要涉及系统规划与建设的法律，系统管理与经营的法律，信息系统安全的法律，用户（自然人或法人）数据的法律保护，电子资金划转的法律认证，计算机犯罪与刑事立法，计算机证据的法律效力等法律问题。同时，还要有法必依，有法必行。

法律是计算机信息系统安全的第一道防线。不难设想，若无这些法律的建设和法律的实施，网络将不成其为网络，信息系统的规划与建设必然是混乱的，信息网络将没有规范的协调的运营管理，数据将得不到有效的保护，电子资金的划转将产生法律上的纠纷，网络将受到黑客的攻击而黑客受不到惩罚。仅仅这些问题的发生，即将使网络无法安全地传递信息，无法起到信息传递通道的作用。

有了相关法律的保障，没有相应的政策，也无法使保障计算机信息系统安全具有可操作性。如美国联邦政府 1996 年发布了 A－130 通告，在附录"联邦政府自动化信息资源安全"政策大纲中，具体阐述了计算机系统的安全对策，可操作性很强。法律、规范、标准、规章形成一个完整的体系，保护计算机信息系统的安全。

2. 安全管理

管理问题包括三个层次的内容：组织建设、制度建设和人员意识。组织建设问题是指有关计算机信息安全管理机构的建设。信息安全的管理包括安全规划、风险管理、应急计划、安全教育培训、安全系统的评估、安全认证等多方面的内容，因此只靠一个机构是没法解决这些问题的。在各信息安全管理机构之间，要有明确的分工，要明确管理机构的职责，还要建立切实可行的规章制度，以保证计算机信息系统安全。如对人的管理，需要解决多人负责、责任到人的问题，任期有限的问题，职责隔离的问题，最小权限的问题。还需要领导的高度重视和群防群治。这需要安全意识的教育和培训，以及对安全问题的高度重视。

为此，要做好计算机信息系统安全保护工作，必须明确以下几个概念：安全是个管理的概念，只有加强管理才能保障安全；安全是一个过程，是动态的，没有一劳永逸的安全措施，要警钟常鸣；安全是相对的，要有风险意识。

在计算机信息系统安全管理方面，安全管理的方法应从系统安全管理五个方面着手，全面进行安全管理，即实体安全管理、行政安全管理、信息流程安全管理、技术安

全管理、安全稽核。

安全管理的核心是人，要提高有关计算机业务人员的思想素质、职业道德和业务素质，因为计算机是由人来操作的，这个问题不解决，其他一切措施再好，也不能保证安全，因此，必须要求主管部门和经营单位从管好计算机业务人员入手，全面加强计算机信息系统的安全管理工作。普遍开展计算机安全教育，提高对计算机信息系统安全保护的认识，逐步建立和完善计算机安全管理机制，是改善和有效实施计算机信息系统安全的极其重要的基础。

3. 安全技术

计算机信息系统安全技术涉及多领域、涵盖多学科。我们可以用下面的等式来描述预防计算机信息系统发生事故，进行安全保护的全过程：

计算机信息系统安全保护 = 事前检查 + 事中防护、监测、控制 + 事后取证。

事前阶段的主要任务是使用自动化的风险评估工具，对计算机信息系统进行预防性检查，及时发现问题，并予以解决。

事中阶段是指计算机信息系统安全事故正在发生的阶段。此阶段的主要目标是提高本系统抗攻击能力，增加黑客攻击难度，加强监控、监测，尽早发现事故苗头，及时中止事故进程，最大限度地压缩安全事故运行时间，将事故损失降到最少。

事后阶段是指计算机信息系统安全事故的进程得到有效控制之后的阶段。此阶段的主要目标是研究事故起因、评估损失、责任追查。核心在于电子数据取证。安全审计信息的采集应该是多层次、多方位、多手段的，并且具有不可抵赖性。

由此可以看出安全技术包含于计算机信息系统安全保护和安全监察的全过程。

4. 计算机信息系统安全矩阵

实体安全、运行安全、信息安全和人员安全，是计算机信息系统安全保护目标的主要内容。每一项安全目标的确实实现，往往都需要采取安全法规、安全技术和安全管理的综合性措施。或者简明地说，为了实现某一项安全指标，能够采取的措施，可能有多种组合，或侧重于安全技术，或偏注于严格的安全管理。

图 1.1 大体上表达了计算机信息系统的安全目标与安全措施的主要内容关系。图中矩阵 A 的所有元素，表示为安全措施的集合，用以实现各个安全目标，称为计算机信息系统安全矩阵，或简称为安全矩阵。

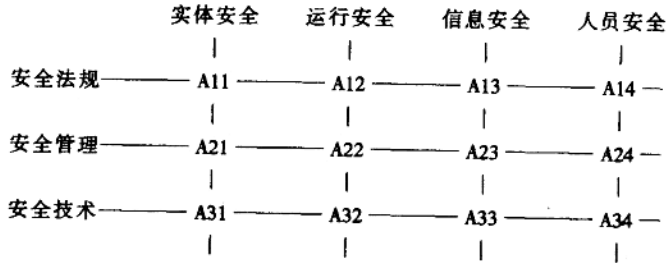

图 1.1 计算机信息系统安全矩阵

在安全矩阵 A：

$$i=\begin{cases}1 & \text{：表示法律规范}\\ 2 & \text{：表示安全管理措施}\\ 3 & \text{：表示安全技术措施}\end{cases}$$

$$j=\begin{cases}1 & \text{：表示实体安全}\\ 2 & \text{：表示运行安全}\\ 3 & \text{：表示信息安全}\\ 4 & \text{：表示人员安全}\end{cases}$$

这些“措施的集合”有着许多各自相对独立的专题、门类，这就是该立体矩阵图的第三维坐标，为使矩阵 图显得简明清晰，未在图中画出，仅作此说明。

（二）计算机信息系统安全保护的基本策略

一切影响计算机信息系统安全的因素，以及保障计算机及其运行的安全措施，都属于计算机安全保护所涉及的内容。

任何危害，都有一个产生、途径、方法和完成的过程。在这全过程的任何环节上，我们都可以采取相应的有力措施，予以制约或制止，避免或减轻遭到的危害。或者说，应当而且可以在计算机安全保护的各个层次上，制止或制约危害的产生，确保计算机信息系统的安全运行。

从宏观上看，可用图 1.2 表示维护计算机信息系统安全的主要逻辑层次。

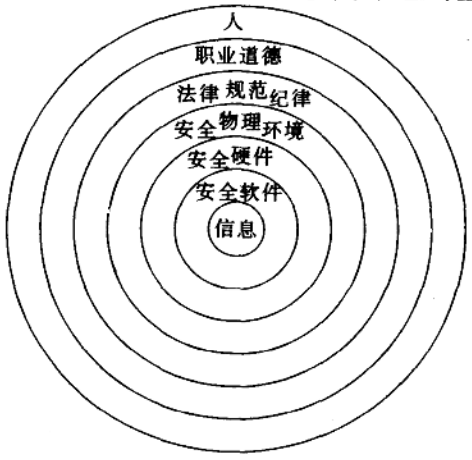

图 1.2 计算机信息系统安全保护逻辑层次

图 1.2 中各层的安全保护之间，是通过界面相互依托、相互支持的；外层向内层提供支持。信息处于被保护的核心，与安全软件和安全硬件均密切相关；人，处于图 1.2 中的最外层，是最需要层层防范的。

无论是整体上，还是每个层次内，不管是安全法规的，或者是安全技术的，之所以能够有效地发挥其应有 的功能，全在于有效的社会公共安全管理和使用单位的内部管理。

很显然，对于各个具体的计算机信息系统而言，既要看到共性，也要注意各自系统面临的具体的可能威胁，以及实际的安全需要和可能，因此，需要和能够采取的适度的