第 1 章

绪　论

信息技术创立、应用和普及是 20 世纪技术革新最伟大的创举之一，借此，人类正在进入信息化社会，人们对信息、信息技术的依赖程度越来越高。与此同时，信息安全问题日渐突出，情况也越来越复杂。

信息安全管理是保障信息系统安全的有力手段，是当今世界各国都在努力推广与应用的重点课题。它涉及的内容广泛，包括技术、方法、保障体系等多方面内容。本章主要阐述信息安全的概念、信息安全管理的概念、信息安全管理的指导原则、信息安全管理的意义、信息安全管理的国内外研究发展，并对本书内容安排进行了说明。

1.1　信息安全

1.1.1　信息安全的现状

由于信息具有易传输、易扩散、易破损的特点，信息资产比传统资产更加脆弱，更易受到损害，信息及信息系统需要严格管理和妥善保护。

1988 年 11 月 2 日，康奈尔大学的研究生罗伯特 · 莫里斯（22 岁）设计了第一个蠕虫程序，设计初始目的是验证网络中自动传播程序的可行性。该程序感染了 6000 台计算机，使互联网不能正常运行，造成的经济损失达 1 亿美元。程序只有 99 行，利用了 UNIX 系统中的缺点，用 Finger 命令查联机用户名单，然后破译用户口令，用 Mail 系统复制、传播本身的源程序，再编译生成代码。莫里斯因此被判 3 年缓刑、罚款 1 万美元、做 400 小时的社区服务。

1998 年 6 月 2 日，首次出现 CIH 的报道。CIH 病毒是由中国台湾大学生陈盈豪编制的，其动机是“为自己设计病毒”。CIH 病毒 1998 年 4 月 26 日发作，可导致主板、硬盘损坏，变种版本极多，危害严重。1999 年 4 月 26 日 CIH 1.2 版本首次大范围爆发全球超过 6000 万台计算机遭到不同程度破坏；2000 年 4 月 26 日 CIH 1.2 版本第二次大范围爆发，全球损失超过 10 亿美元；2001 年 4 月 26 日 CIH 第三次大范围爆发，仅北京就有超过 6000 台计算机遭 CIH 破坏，瑞星修复硬盘数量当天接近 400 块。

2000 年 5 月 4 日，“爱虫（LOVE BUG）”病毒大爆发。主要表现是邮件群发、修改文件、消耗网络资源。“爱虫”大爆发两天之后，全球约有 4500 万台计算机被感染，造成的损失已经达到 26 亿美元。此后几天里，“爱虫”病毒所造成的损失还将以每天 10 亿～15 亿美元的速度增加。

近两年也发生了几起重大的信息安全事件，2014 年 1 月 21 日，中国互联网出现大面积 DNS 解析故障。2014 年 10 月 2 日，摩根大通银行承认 7600 万家庭和 700 万小企业的相关信息被泄露。

身在南欧的黑客取得摩根大通数十个服务器的登入权限，偷走银行客户的姓名、住址、电话号码和电邮地址等个人信息，与这些用户相关的内部银行信息也遭到泄露。受影响者人数占美国人口的1/4。2015 年 4 月，超 30 省市曝安全管理漏洞，数千万社保用户敏感信息或遭泄露。从补天漏洞响应平台获得的数据显示，目前围绕社保系统、户籍查询系统、疾控中心、医院等大量曝出高危漏洞的省市已经超过 30 个，仅社保类信息安全漏洞统计就达到 5279.4 万条，涉及人员数量达数千万，其中包括个人身份证、社保参保信息、财务、薪酬、房屋等敏感信息。

不断发生的信息安全事件，对信息安全提出了严峻的挑战。据统计，全球平均 20s 就发生一次计算机病毒的入侵；互联网上的防火墙大约 25%被攻破；窃取商业信息的事件平均以每月 260%的速度增加；约 70%的网络主管报告因机密信息泄露而受到损失。国家与国家之间的信息战问题更是关系到国家的根本安全问题。信息安全已成为信息社会重要的研究课题。

1.1.2 信息安全的概念、特点及意义

1．信息安全的概念

关于信息安全，不同组织有不同的定义，国际标准化组织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和恶意的原因而遭到破坏、更改和泄露 ”。在我们常见的很多信息安全文献中定义信息安全主要包括 3 个方面：机密性、完整性、可用性。目前，信息安全的内涵已从传统的机密性、完整性和可用性 3 个方面扩展到机密性、完整性、可用性、真实性、抗抵赖性、可靠性、可控性等更多领域。各信息安全属性的含义如下。

（1）机密性：信息不泄漏给非授权的用户、实体或者过程的特性。

（2）完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

（3）可用性：可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。

（4）真实性：信息所反映内容与客观事实是否一致的特性。

（5）抗抵赖性：证实行为或事件已经发生的特性，以保证事件或行为不能被抵赖。

（6）可靠性：保持持续的预期行为及结果的特性。

（7）可控性：对信息的传播及内容具有控制能力，访问控制即属于可控性。

2．信息安全的特点

信息安全在技术发展和应用过程中，表现出以下重要特点。

（1）必然性。当今的信息系统日益复杂，其中必然存在系统设计、实现、内部控制等方面的弱点。如果不采取适当的措施应对系统运行环境中的安全威胁，信息资产就可能会遭受巨大的损失甚至威胁到国家安全。所以，信息安全已引起许多国家、特别是发达国家的高度重视，他们在这个领域投入了大量的人力、物力、财力，以期提高本国的信息安全水平。

（2）配角特性。信息安全建设在信息系统建设中角色应该是陪衬，安全不是最终目的，得到安全可靠的应用和服务才是安全建设的最终目的。不能为了安全而安全，安全的应用是先导。

（3）动态性。信息安全威胁会随着技术的发展、周边应用场景的变化等因素而发生变化，新的安全威胁总会不断出现。所以，信息安全建设是一个动态的过程，不能指望一项技术、一款产品或一个方案就能一劳永逸地解决组织的安全问题，信息安全是一个动态、持续的过程，必须能根据风险变化及时调整安全策略。一成不变的静态策略，在信息系统的脆弱性，以及威胁技术发生变化时将变得毫无安全作用，因此安全策略，以及实现安全策略的安全技术和安全服务，应具有“ 风险监测—实时响应—策略调整—风险降低 ”的良性循环能力。

3．信息安全的意义

信息时代，信息安全不仅关系信息自身的安全，更是对国家安全具有重大战略价值。

（1）信息安全的政治意义。

首先，在任何国家，信息安全都是国家安全战略的重要组成部分，尤其是信息技术的发展及信息战的广泛应用，信息安全作为夺取战略制高点的关键因素越来越被各国政府重视。

其次，在全球一体化的今天，常规的战争形态已经慢慢退出历史舞台，国与国之间的战争形式表现在更早获取和掌握对方的各方面情报信息，进行多种形式的打击（如网络战、电子战、经济战、舆论战等），这都是为了获取对本国的最大经济利益和政治利益。而在这个过程中，信息安全被赋予了格外的关注。

（2）信息安全的经济意义。

经济安全的实质是一国最为根本的经济利益不受侵害，通常一国的经济安全取决于该国产业的竞争能力。信息或信息化对于我国产业竞争能力的提升具有战略价值。这不仅在于信息产业已成为支柱产业，更在于信息或信息化已经成为产业总体竞争力提升的基础性手段和核心标志。农业竞争力的提升对信息化的依赖突出体现在，包括物质装备、种植技术、经营管理、资源环境、农民素质等的现代化，只有依托信息化才能真正实现。工业或工业企业，要在激烈的战争中立于不败之地，必须从整体上实现信息化。

由于信息技术的开放性与经济主体利益的冲突性并存，现实的信息系统同样存在着安全风险。信息或信息化有可能对我国的经济安全水平造成严重的冲击，蕴藏着巨大的风险。确保信息安全有助于规避经济安全风险或最大限度地减少这类风险。

（3）信息安全与社会稳定的意义。

当前，我国正处在全面建设小康社会、构建社会主义和谐社会的重要阶段。改革开放 30 多年来，我国的综合国力显著增强，经济稳步增长，社会政治稳定，人民安居乐业，为推动科学发展、促进社会和谐营造出良好的社会环境。但也要清醒地看到，天下并不太平，危害社会稳定、国家安全和社会公共秩序的煽动性信息大量存在。

信息的泄露所带来的已不仅仅是经济上的损失，在一些地方，侵害公民个人信息犯罪与绑架、敲诈勒索、暴力追债等黑恶犯罪合流。维护信息安全对于保护公民安全、维护法律尊严和社会稳定，都具有重要意义。

1.1.3　信息安全威胁

信息化进程在加快，信息化的覆盖面在扩大，信息安全问题也就随之日益增多和复杂，其造成的影响和后果也会不断扩大和更趋严重。信息安全面临的威胁主要来自以下 3 个方面。

1．日益严重的计算机病毒

计算机病毒本身是一种程序，通过信息流动感染计算机的操作系统，最终目的是侵入对方的信息系统，窃取相关的信息资料。其主要特征有以下几个。

第一，破坏性强。计算机病毒可以造成操作系统和应用系统的瘫痪并破坏侵入对象的信息资源，因此具有很强的破坏性。通过感染计算机的硬盘，可能造成分区中的某些区域上内容的损坏，使计算机瘫痪，无法正常工作。

第二，传播性强。计算机病毒通过网络和信息手段进行传播，其传播瞬间可达，扩散迅速。

第三，扩散面广。由于信息技术的巨大覆盖性和扩散性，通过网络传播能够在很短的时间内扩散到网络节点的其他计算机，而一旦网络服务器被感染，其扩散面将更加广泛，清除病毒所需的时间将是单机的几十倍以上。

伴随着计算机技术的提高，近年来计算机病毒也越来越强大，蠕虫病毒具有很快的传播速度和很强大的破坏力，木马病毒能够对受感染计算机实施远程控制并盗取重要信息，虽然现有的杀毒软件能够查杀一部分病毒，但是不断产生的新型病毒还是能够绕过很多杀毒软件的查杀，对目标对象实施感染。同时，计算机病毒还成为交易商品可以进行网上买卖且呈现公开化的趋势。可以说，日益严重的计算机病毒已经对网络信息安全造成了巨大的威胁。以“震荡波”病毒为例，“震荡波”（Sasser）病毒利用微软公布的 LSASS 漏洞进行传播，通过 Windows 2000/XP 等操作系统，开启上百个线程去攻击其他网上的用户，造成机器运行缓慢、网络堵塞。由于其隐蔽性，在一周之内就感染了全球 1800 多万台计算机。“震荡波”病毒在全球带来的损失超过 5 亿美元。根据有关统计数据显示，“震荡波”造成 73%的中毒计算机不得不申请专业防毒公司解救，63%的中毒者工作受到严重影响，30%的人至少花费 10 小时去除病毒，同时估计全球范围为处理“震荡波”病毒造成的计算机损害要花 9.97 亿美元。

利用病毒、木马技术传播垃圾邮件和进行网络攻击、破坏的事件呈上升趋势。计算机病毒主要为获取受感染者的密码和账号信息，从中获取利益。计算机病毒的入侵主要为盗取用户敏感信息，特别是涉及账号、密码等重要经济信息成为网络非法入侵的主要目标。

2．人为的因素

相对物理实体和硬件系统及自然灾害而言，精心设计的人为攻击威胁最大。人的因素最为复杂，思想最为活跃，不能用静止的方法和法律、法规加以防护，这是信息安全所面临的最大威胁。

人为因素分为两种情况：第一种为用户自己的无意操作失误而引发的网络安全，如管理员安全管理不当造成安全漏洞，用户安全意识淡薄，将自己的账户随意转借他人或与别人共享等；第二种为人为的恶意破坏，人为恶意攻击可以分为主动攻击和被动攻击。主动攻击的目的在于篡改系统中信息的内容，以各种方式破坏信息的有效性和完整性。被动攻击的目的是在不影响网络正常使用的情况下，进行信息的截获和窃取。总之，不管是主动攻击还是被动攻击，都给信息安全带来巨大损失。攻击者常用的攻击手段有木马、黑客后门、网页脚本、垃圾邮件等。

网络黑客（Hacker）是专业进行网络计算机入侵的人员，通过入侵计算机网络窃取机密数据和盗用特权，或进行文件破坏，或使系统功能得不到充分发挥直至瘫痪。从世界范围看，黑客的攻击手段在不断地更新，几乎每天都有不同系统安全问题出现。黑客就是利用网络安全的漏洞，尝试侵入其聚焦目标的。随着计算机和网络技术的普及，世界范围内的黑客数量日益庞大，黑客的对象也越来越趋向难度更高的政府、情报部门、大型企业、银行等网站。同时，黑客之间也出现了协同作战的现象，黑客群体呈现集团化、组织化、政治化，甚至国家行为化的趋势。黑客攻击往往呈现较高的智能性和很强的隐蔽性等特点。从智能性上看，黑客普遍具有相当高水平的计算机操作技术，能够绕过所侵入系统的防火墙和拦截软件；从隐蔽性上看，黑客利用计算机作为窃取信息的载体，并以计算机作为入侵的目标，通过编辑程序达到入侵目的，而非直接入侵所要侵入的地点。黑客的行为虽然一般比较隐蔽，但造成的危害一般比较巨大。从我国的实际情况来看，除传统领域的信息安全受到危害外，更为隐蔽和难以追查的信息安全非法手段是通过一些非政府组织、极端宗教组织等进行的信息安全违法行为，这些行为往往具有手段隐蔽、技术手段高等特点，因此在追查方面也更加具有难度，同时在破坏程度上也更加严重。

3．信息安全管理自身的不足

面对复杂、严峻的信息安全管理形势，根据信息安全风险的来源和层次，有针对性地采取技术、管理和法律等措施，谋求构建立体的、全面的信息安全管理体系，已逐渐成为共识。与反恐、环保、粮食安全等安全问题一样，信息安全也呈现出全球性、突发性、扩散性等特点。信息及网络技术的全球性、互联性、信息资源和数据共享性等，又使其本身极易受到攻击，攻击的不可预测性、危害的连锁扩散性大大增强了信息安全问题造成的危害。信息安全管理已经被越来越多的国家所重视。

与发达国家相比，我国的信息安全管理研究起步比较晚，基础性研究较为薄弱。研究的核心仅仅停留在信息安全法规的出台、信息安全风险评估标准的制定及一些信息安全管理的实施细则，应用性研究、前沿性研究不强。这些研究没有从根本上改变我们管理底子薄、漏洞多的现状。

1.2　信息安全管理

1.2.1　信息安全管理的概念

信息是一个组织的血液，它的存在方式各异。可以是打印、手写，也可以是电子、演示和口述的。当今商业竞争日趋激烈，来源于不同渠道的威胁，威胁到信息的安全性。这些威胁可能来自内部，也可能来自外部，可能是意外的，还可能是恶意的。随着信息存储、发送新技术的广泛使用，信息安全面临的威胁也越来越严重了。

信息安全的建设过程是一个系统工程，它需要对信息系统的各个环节进行统一的综合考虑、规划和架构，并需要兼顾组织内外不断发生的变化，任何环节上的安全缺陷都会对系统构成威胁。这点可以借用管理学上的木桶原理加以说明。木桶原理是指：一个木桶由许多木板组成，如果木板的长短不一，那么木桶的最大容量取决于最短的那块木板。这个原理可适用信息安全。一个组织的信息安全水平将由与信息安全有关的所有环节中最薄弱的环节决定。信息从产生到销毁，其生命周期过程中包括了产生、收集、加工、交换、存储、检索、存档、销毁等多个事件，表现形式和载体会发生各种变化，这些环节中的任何一个环节都可能影响整体信息安全水平。要实现信息安全目标，一个组织必须使构成安全防范体系的这只“木桶”的所有木板都要达到一定的长度。

由于信息安全是一个多层面、多因素、综合和动态的过程，如果组织凭着一时的需要，想当然制定一些控制措施和引入某些技术产品，都难免存在挂一漏万、顾此失彼的问题，使得信息安全这只“木桶”出现若干“短板”，从而无法提高安全水平。正确的做法是遵循国内外相关信息安全标准和最佳实践的过程，考虑到组织信息安全各个层面的实际需求，在风险分析的基础上引入恰当的控制，建立合理的安全管理体系，从而保证组织赖以生存的信息资产的机密性、完整性和可用性；另一方面，这个安全体系还应当随着组织环境的变化、业务发展和信息技术提高而不断改进，不能一劳永逸，一成不变。因此，实现信息安全是一个需要完整体系来保证的持续过程。这就是组织需要信息安全管理的基本出发点。

所谓管理，是指管理主体组织并利用其各个要素（人、财、物、信息和时空），借助管理手段，完成该组织目标的过程。

（1）管理主体是一个组织，这个组织可能是国家，可以是一个单位；也可能是一个正式组织或非正式组织。

（2）管理主体包含 5 个方面的要素：人（决策者、执行者、监督者）、财（资金）、物（土地、生产设备及工具、物料等）、信息（管理机制、技术与方法、管理用的各种信息等）、时空（时点和持续时间、地理位置及空间范围）。

（3）管理的手段包括 5 个方面：强制（战争、政权、暴力、抢夺等）、交换（双方意愿交换）、惩罚（包括物质性的和非物质性；包括强制、法律、行政、经济等方式）、激励、沟通与说服。

（4）管理的过程包括 7 个环节：管理规则的确定（组织运行规则，如章程及制度等）、管理资源的配置（人员配置及职责划分与确定、设备及工具、空间等资源配置与分配）、目标的设立与分解（如计划）、组织与实施、过程控制（检查、监督与协调）、效果评价、总结与处理（奖惩）。

信息安全管理是组织为实现信息安全目标而进行的管理活动，是组织完整的管理体系中的一个重要组成部分，是为了保护信息资产的安全，指导和控制组织的关于信息安全风险的互相协调的活动。

信息安全管理在对组织内部和外部信息的有效管理基础上，为企业、单位和组织提供决策支持的工作。

在当今全球一体化的商业环境中，信息的重要性被广泛接受，信息系统在商业和政府组织中得到了真正的广泛的应用。许多组织对其信息系统不断增长的依赖性，加上在信息系统上运作业务的风险、收益和机会，使得信息安全管理成为企业管理越来越关键的一部分。管理高层需要确保信息技术适应企业战略，企业战略也恰当利用信息技术的优势。

1.2.2 信息安全管理的基本内容

信息系统的安全管理涉及与信息系统有关的安全管理及信息系统管理的安全两个方面。这两方面的管理又分为技术性管理和法律性管理两类。其中技术性管理以 OSI 安全机制和安全服务的管理及对物理环境的技术监控为主，法律性管理以法律法规遵从性管理为主。信息安全管理本身虽并不完成正常的业务应用通信，却是支持与控制这些通信的安全所必需的。

由信息系统的行政管理部门依照法律并结合本单位安全实际需要而强加给信息系统的安全策略可以是各种各样的，信息安全管理活动必须支持这些策略。受同一个机构管理并执行同一个安全策略的多个实体构成的集合有时称为“安全域”。安全域及其相互作用是一个值得进一步研究的重要领域。

信息系统管理的安全包括信息系统所有管理服务协议的安全及信息系统管理信息的通信安全，它们是信息系统安全的重要部分。这一类安全管理将借助对信息系统安全服务与机制做适当的选取，以确保信息系统管理协议与信息获得足够的保护。

在信息安全管理的技术性管理中，为了强化安全策略的协调性和安全组件之间的互操作性，设计了一个极为重要的基本概念，即用于存储和交换开放系统所需的与安全有关的全部信息的安全管理信息库（SMIB）。SMIB 是一个分布式信息库。在实际中，SMIB 的某些部分可以与 MIB 结合成一体，也可以分开。SMIB 有多种实现办法，如数据表、文件及嵌入到实开放系统软件或硬件中的数据或规则。

安全管理协议及传送这些管理信息的通信信道，可能遭受攻击。所以应特别对安全管理协议及其协议数据加以保护，其保护的强度通常不低于为业务应用通信提供的安全保护的强度。

安全管理可以使用 SMIB 信息在不同系统的行政管理机构之间交换与安全有关的信息。在某些情况下，与安全有关的信息可经由非自动信息通信通道传递，局部系统的管理者也可采用非标准化方法来修改 SMIB。在另外一些情况下，可能希望通过自动信息通信通道在两个安全管理机构之间传递信息。在获得安全管理者授权后，该安全管理将使用这些通信信息来修改 SMIB。修改 SMIB，必须先得到安全管理者的授权。

1.3 信息安全管理的指导原则

1.3.1 策略原则

信息安全管理的基本原则如下。

1．以安全保发展，在发展中求安全

信息安全的目的是通过保护信息系统内有价值的资产，如数据、硬件、软件和环境等以实现信息系统的健康、有序和稳定运行，促进社会、经济、政治和文化的发展。没有安全保证的信息化，以及牺牲信息化发展来换取安全，是两种必须摒弃的错误做法。科学的安全发展观是在安全意识上全面提高对信息安全保障认识的同时，采用渐进的适度安全策略来保证和推进信息化的发展，并通

过信息化的发展为信息安全保障体系的逐步完善提供充足的人力、财力和物力支持。

2．受保护资源的价值与保护成本平衡

信息安全的成本和效益比应该在货币和非货币两个层面上进行评估，以保证将成本控制在预期的范围内。

3．明确国家、企业和个人对信息安全的职责和可确认性

应该明确表述与信息系统相关的所有者、管理者、经营者、供应商及使用者应该承担的安全职责和可确认性。

4．信息安全需要积极防御和综合防范

信息安全需要综合治理的方法，坚持保护与监管相结合、技术措施与管理并重的方针，综合治理方法将延伸到信息系统的整个生命期。

5．定期评估信息系统的残留风险

信息系统及其运行环境是动态变化的，一劳永逸的信息系统安全解决方案是不存在的。因此必须定期评估信息系统的残留风险，并以此调整安全策略。

6．综合考虑社会因素对信息安全的制约

信息安全受到很多社会因素的制约，如国家法律、社会文化和社会影响等。安全措施的选择和实现还应该综合考虑法律框架下信息系统所有者与使用者、所有者和社会各方面之间的利益平衡。

7．信息安全管理体现以人为本

信息安全管理要体现人性化、社会公平和交换平等的价值观念。

1.3.2　工程原则

为了指导信息安全工程的组织和实施，信息安全工程应遵循 6 类基本原则，即基本保证、适度安全、实用和标准化、保护层次化和系统化、降低安全度和安全设计结构化。这些原则简单明了，可应用于信息系统的安全规划、设计、开发、运行、维护管理和报废处理等多个环节。

1．基本保证

（1）信息系统安全设计前应制定符合本系统实际的安全目标和策略。

（2）将安全作为整个系统设计不可分割的部分。

（3）识别信息及信息系统资产，以此作为风险分析和安全需求分析的对象。

（4）划分安全域。

（5）确保开发者受过软件安全开发的良好训练。

（6）确保信息系统用户的职业道德和安全意识的持续培训。

2．适度安全

（1）通过对抗、规避、降低和转移风险等方式将风险降低到可接受的水平，不追求绝对的或过度安全的目标。

（2）安全的标志之一是系统可控。

（3）在减小风险、增加成本开销和降低某些操作有效性之间进行折中，避免盲目地追求绝对安全目标。

（4）采用剪裁方式选择系统安全措施，以满足组织的安全目标。

（5）保护信源到信宿全程的机密性、完整性和可用性。

（6）在必要时自主开发非卖品以满足某些特殊的安全需求，将残留风险保持在可接受水平。

（7）预测并对抗、规避、降低和转移各种可能的风险。

3．实用和标准化

（1）尽可能采用开放的标准化技术或协议，增强可移植性和互操作性。

（2）使用便于交流的公告语言进行安全需求的开发。

（3）设计的新技术安全机制或措施，要确保系统平稳过渡，并保证局部采用的新技术不会引起系统的全局性调整，或引发新的脆弱点。

（4）尽量简化操作，以减少操作带来新的风险。

4．保护层次化和系统

（1）识别并预测普遍性故障和脆弱性。

（2）实现分层的安全保护（确保没有遗留的脆弱点）。

（3）设计和运行的信息系统对入侵和攻击应具有必要的检测、响应和恢复能力。

（4）提供对信息系统各个组成部分的体系性保障，使信息系统面对预期的威胁具有持续阻止、对抗和恢复能力。

（5）容忍可以接受的风险，拒绝绝对安全的策略。

（6）将公共可访问资源与关键业务资源进行物理/逻辑隔离。

（7）采用物理或逻辑方法将信息系统的局域网络与公共基础设施相隔离。

（8）设计并实现审计机制，以检测非授权和越权使用系统资源，并支持事故调查和责任确认。

（9）开发意外事故处置或灾难恢复规程，并组织学习和演练。

5．降低复杂度

（1）安全机制或措施力求简单实用。

（2）尽量减少可信系统的要素。

（3）实现访问的最小特权控制。

（4）消除不必要的安全机制或安全服务冗余。

（5）“开机—处理—关机”全程安全控制。

6．安全设计机构化

（1）通过对物理/逻辑的安全措施进行合理组合实现系统安全设计的优化。

（2）所配置的安全措施或安全服务可作用于多个域。

（3）对用户或进程使用鉴别技术，以确保在域内和跨域间的访问权控制。

（4）对实体进行标识以确保责任的可追究性。

1.4　信息安全管理的意义

信息安全管理通过维护信息的机密性、完整性和可用性等，来管理和保护信息资产的一项体制，是对信息安全保障进行指导、规范和管理的一系列活动和过程。在当今全球一体化的商业环境中，信息的重要性被广泛接受，信息系统在商业和政府组织中得到了真正的广泛的应用。许多组织对其信息系统不断增长的依赖性，加上在信息系统上运作业务的风险、收益和机会，使得信息安全管理成为企业管理越来越关键的一部分。管理高层需要确保信息技术适应企业战略，企业战略也恰当利用信息技术的优势。

但现实世界的任何系统都是一串复杂的环节，安全措施必须渗透到系统的所有地方，其中一些甚至连系统的设计者、实现者和使用者都不知道。因此，不安全因素总是存在。没有一个系统是完美的，没有一项技术是灵丹妙药。

目前业界普遍认为，信息安全是政府和企业必须携手面对的问题。政府和企业管理层有责任确保为所有使用者提供一个安全的信息系统环境，而且，政府部门和企业在认识到安全的信息系统好处的同时，应该自我保护以避免使用信息系统时的固有风险。

中国工程院院长徐匡迪曾指出：“没有安全的工程就是豆腐渣工程”。今年我国接连不断地出现程度不同的信息安全事件，这些事件不仅仅是简单的信息系统瘫痪的问题，其直接后果是导致巨

大的经济损失，还造成了不良的社会影响。如果说经济损失还能弥补，那么由于信息网络的脆弱性而引起的公众对网络社会的诚信危机则不是短时期内可能恢复的。

我国政府主管部门及各行各业已经认识到了信息安全的重要性。政府部门开始出台一系列相关策略，直接牵引、推进信息安全的应用和发展。由政府主导的各大信息系统工程和信息化程度要求非常高的相关行业，也开始出台对信息安全技术产品的应用标准和规范。国务院信息化工作小组颁布的《关于我国电子政务建设指导意见》也强调指出了电子政务建设中信息系统安全的重要性；中国人民银行正在加紧制定网上银行系统安全性评估指引，并明确提出对信息安全的投资要达到 IT 总投资的 10%以上，而在其他一些关键行业，信息安全的投资甚至已经超过了总 IT 预算的 30%～50%。

我们回头来看，政府和各行各业对信息安全的重要性有了认识，相关的标准规范正在形成，投资力度在加大，安全技术、产品、市场在发展，多数企业机构正在制定符合不同业务信息系统和网络安全等级需要的综合性安全策略和计划。那么，我们为什么依然没有安全感呢？到底需要什么样的方法或机制来管理或治理信息安全呢？经过近一年对国内外信息安全和最佳实务的研究，我们认为关键是要建立一套能够涵盖组织信息安全的制度安排机制，它包括治理机制和治理结构，这种制度安排通过建立和维护一个框架来保证信息安全战略和组织的业务目标精确校准，并且和相关的法律和规范一致。所以有效的信息安全管理是非常必要的。

1.5　信息安全管理的国内外研究发展

1.5.1　国内信息安全管理现状

1．我国已初步建成了国家信息安全组织保障体系

国务院信息办专门成立了网络与信息安全领导小组，各省、市、自治州也设立了相应的管理机构。2003 年 7 月，国务院信息化领导小组通过了《关于加强信息安全保障工作的意见》，同年 9 月，中央办公厅、国务院办公厅转发了《国家信息化领导小组关于加强信息安全保障工作的意见》，把信息安全提到了促进经济发展、维护社会稳定、保障国家安全、加强精神文明建设的高度，并提出了“ 积极防御，综合防范 ”的信息安全管理方针。

2003 年 7 月成立了国家计算机网络应急技术处理协调中心，专门负责收集、汇总、核实、发布权威性的应急处理信息。2001 年 5 月成立了中国信息安全产品测评认证中心和代表国家开展信息安全测评认证工作的职能机构，还建立了依据国家有关产品质量认证和信息安全管理的法律法规管理和运行国家信息安全测评认证体系。

2．制定和引进了一批重要的信息安全管理标准

为了更好地推进我国信息安全管理工作，公安部主持制定、国家质量技术监督局发布了中华人民共和国国家标准 GB 17895—1999《计算机信息系统安全保护等级划分准则》《信息系统安全等级保护基本要求》等技术标准和 GB/T 20269—2006《信息安全技术 信息系统安全管理要求》、GB/T 20282—2006《信息安全技术 信息系统安全工程管理要求》《信息系统安全等级保护基本要求》等管理规范，并引进了国际上著名的 ISO/IEC 17799:2000《信息技术—信息安全管理实施规则》、BS 7799—2:2000《信息安全管理体系实施规范》等信息安全管理标准。

3．制定了一系列必需的信息安全管理的法律法规

从 20 世纪 90 年代初起，为配合信息安全管理的需要，国家相关部门、行业和地方政府相继制定了《中华人民共和国计算机信息网络国际联网管理暂行规定》《商用密码管理条例》《互联网信息服务管理办法》《计算机信息网络国际联网安全保护管理办法》《中华人民共和国电子签名法》等有关信息安全管理的法律法规文件。

4．信息安全风险评估工作已经得到重视和开展

风险评估成为信息安全管理的核心工作之一。2003 年 7 月，国务院信息化工作办公室（以下简称国信办）信息安全风险评估课题组就启动了信息安全风险评估相关标准的编制工作，国家铁路系统和北京移动通信公司作为先行者已经完成了信息安全风险评估试点工作，国家其他关键行业或系统（如电力、电信、银行等）也将陆续开展这方面的工作。

1.5.2 我国信息安全管理存在的问题

随着信息技术在国民生活与经济中的地位越来越重要，我国信息安全管理得到了人们的重视，相继出台了一系列的法律法规，但信息安全管理仍存在着许多的问题。

（1）信息安全管理现状比较混乱，缺乏一个国家层面上的整体策略，实际管理力度不够，政策执行和监督力度也不够。

（2）具有我国特点的、动态的和涵盖组织机构、文件、控制措施、操作过程和程序及相关资源等要素的信息安全管理体系还未建立起来。

（3）具有我国特点的信息安全风险评估标准体系还有待完善，信息安全的需求难以确定，缺乏系统、全面的信息安全风险评估和评价体系，以及全面、完善的信息安全保障体系。

（4）信息安全意识缺乏，普遍存在重产品、轻服务，重技术、轻管理的思想。

（5）专项经费投入不足，管理人才极度缺乏，基础理论研究和关键技术薄弱，严重依靠国外。

（6）技术创新不够，信息安全管理产品水平和质量不高。

（7）缺乏权威、统一、专门的组织、规划、管理和实施协调的立法管理机构，致使我国现有的一些信息安全管理方面的法律法规层次不高，真正的法律少，行政规章多，结构不合理，不成体系；执法主体不明确，多头管理，政出多门、各行其是，规则冲突，缺乏可操作性，执行难度较大，有法难依；数量上不够，内容上不完善，制定周期太长，时间上滞后，往往无法可依；监督力度不够，有法不依、执法不严；缺乏专门的信息安全基本大法，如信息安全法和电子商务法等；缺乏民事法方面的立法，如互联网隐私法、互联网名誉权、网络版权保护法等；公民的法律意识较差，执法队伍薄弱，人才匮乏。

（8）我国自己制定的信息安全管理标准太少，大多沿用国际标准。在标准的实施过程中，缺乏必要的国家监督管理机制和法律保护，致使有标准企业或用户可以不执行，而执行过程中出现的问题得不到及时、妥善解决。

1.5.3 国外信息安全管理现状

信息化发展比较好的发达国家，特别是美国，非常重视国家信息安全的管理工作。美、俄、日等国家都已经或正在制定自己的信息安全发展战略和发展计划，确保信息安全沿着正确的方向发展。美国信息安全管理的最高权力机构是美国国土安全局，分担信息安全管理和执行的机构有美国国家安全局、美国联邦调查局、美国国防部等，主要是根据相应的方针和政策结合自己部门的情况实施信息安全保障工作。2000 年年初，美国出台了计算机空间安全计划，旨在加强关键基础设施、计算机系统网络免受威胁的防御能力。2000 年 7 月，日本信息技术战略本部及信息安全会议拟定了信息安全指导方针。2000 年 9 月俄罗斯批准了《国家信息安全构想》，明确了保护信息安全的措施。

美、俄、日均以法律的形式规定和规范信息安全工作，对有效实施安全措施提供了有力保证。2000 年 10 月，美国的电子签名法案正式生效。2000 年 10 月美参议院通过了《互联网网络完备性及关键设备保护法案》。日本于 2000 年 6 月公布了旨在对付黑客的《信息网络安全可靠性基准》的补充修改方案。2000 年 9 月，俄罗斯实施了关于网络信息安全的法律。

国际信息安全管理已步入标准化与系统化管理时代。在 20 世纪 90 年代之前，信息安全主要依

靠安全技术手段与不成体系的管理规章来实现。随着 20 世纪 80 年代 ISO 9000 质量管理体系标准的出现及随后在全世界的推广应用，系统管理的思想在其他领域也被借鉴与采用，信息安全管理也同样在 20 世纪 90 年代步入了标准化与系统化的管理时代。1995 年英国率先推出了 BS 7799 信息安全管理标准，该标准于 2000 年被国际标准化组织认可为国际标准 ISO/IEC 17799。现在该标准已引起许多国家与地区的重视，在一些国家已经被推广与应用。组织贯彻实施该标准可以对信息安全风险进行安全系统的管理，从而实现组织信息安全。其他国家及组织也提出了很多与信息安全管理相关的标准。

1.6　本书内容安排

第 1 章为绪论。主要阐述信息安全管理的概念、信息安全管理的指导原则、信息安全管理的意义、信息安全管理的国内外研究发展等。

第 2 章为信息安全管理标准与法律法规。分别介绍信息安全风险评估标准、我国信息系统等级保护标准、信息安全管理体系标准、ISO/IEC 27000 系列标准、信息安全法律法规等。

第 3 章为信息安全管理体系。主要介绍 ISMS 实施方法与模型、ISMS 实施过程，ISMS、等级保护、风险评估三者关系，以及国外的 ISMS 实践等内容。

第 4 章为信息安全风险评估。信息安全风险评估是信息安全管理的基本手段，也是信息安全管理的核心内容。本章对信息安全风险评估的概念、策略、流程，以及方法进行详细阐述，并通过一简单案例说明风险评估过程。

第 5 章为信息系统安全测评。主要介绍信息系统安全测评原则、要求及测评的流程，另外还介绍了信息系统安全管理测评，以及信息安全等级保护与等级测评。最后给出一个等级测评的实例。

第 6 章为业务连续性与灾难恢复。首先介绍业务连续性的概念、业务连续性管理体系，以及业务连续性管理中的部分重要环节；接着引出业务连续中的重要内容——灾难恢复和数据备份，并结合国家标准 GB/T 20988—2007《信息安全技术信息系统灾难恢复规范》介绍了灾难恢复的核心内容。

第 7 章为信息系统安全审计。介绍了信息系统安全审计的基本概念、关键技术和相关标准，另外还介绍了将信息安全审计用于计算机犯罪追踪取证的计算机取证。

第 8 章为网络及系统安全保障机制。概要介绍了身份认证技术、网络边界及通信安全技术、网络入侵检测技术、计算机环境安全技术、虚拟化安全防护技术。

本章小结

本章主要介绍信息安全、信息安全管理的概念，并给出信息安全管理的指导原则，以及信息安全管理的意义。并详细介绍了信息安全管理的国内外研究发展现状。最后给出全书的章节安排。

信息安全管理是保障信息系统安全的有力手段，是当今世界各国都在努力推广与应用的重点课题。我国在信息安全管理方面还不成熟，尚存在诸多问题，有待进一步加强。

习题

1. 目前，信息安全的内涵已从传统领域扩展到哪些领域？
2. 信息安全在技术发展和应用过程中，表现出哪些重要特点？
3. 简述信息系统的安全管理涉及信息系统的两个方面。
4. 什么是信息安全管理？
5. 国内信息安全管理现状是什么？