信息安全导论

目　录

第 1 章　信息化发展与信息安全

本章要点

- 信息化发展与信息安全的关系
- 信息安全概念的演变
- 信息安全的非传统安全特征
- 我国信息安全保障工作整体概况

1.1　信息化发展

纵观世界近几百年的历史，可以看到，现代化是一个过程，其内涵是随着人类社会经济的发展而不断演化的。自 18 世纪 60 年代英国产业革命以后，工业化一直是现代化的核心内容。然而，随着 20 世纪下半叶微电子技术和信息产业的出现和快速发展，信息化大潮汹涌而至，信息技术正在使人们的生产和生活发生质的变化，全面转向信息化时代。所谓信息化，是充分利用信息技术，开发利用信息资源，促进信息交流和知识共享，提高经济增长质量，推动经济社会发展转型的历史进程。

20 世纪 90 年代以来，信息技术不断创新，信息产业持续发展，信息网络广泛普及，信息化成为全球经济社会发展的显著特征，并逐步向一场全方位的社会变革演进。进入 21 世纪，信息化对经济社会发展的影响更加深刻。广泛应用、高度渗透的信息技术正孕育着新的重大突破。信息资源日益成为重要生产要素、无形资产和社会财富。信息网络更加普及并日趋融合。信息化与经济全球化相互交织，推动着全球产业分工深化和经济结构调整，重塑着全球经济竞争格局。互联网加剧了各种思想文化的相互激荡，成为信息传播和知识扩散的新载体。电子政务在提高行政效率、改善政府效能、扩大民主参与等方面的作用日益显著。信息化使现代战争形态发生重大变化，成为世界新军事变革的核心内容。

随着信息化发展，信息安全问题开始出现，两者如影相随。同时，信息安全的特点、规律和造成的影响也会随着信息化发展的不同阶段而有所不同。总的趋势是，信息化进程加快，信息化覆盖面扩大，信息安全问题也就会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。没有信息化，就不会产生复杂的信息安全问题，但如果因信息安全问题而拒绝信息技术的广泛应用，则会使我们丧失发展的机遇，国家将因此处于危险的边缘，因为不发展才是最大的不安全。唯有将信息安全置于信息化发展的宏观环境之中，才能深刻认识其规律和内涵，才能有效地解决信息安全问题。

1.1.1　信息化对我国的重要影响

当前，信息技术已经成为最活跃的生产力要素，成为影响国家综合实力和国际竞争力的关键因素，各国都在通过积极发展信息技术及其产业，抢占世界经济竞争的制高点。我国党和政府一直高度重视信息化工作。20 世纪 90 年代，相继启动了以“金关”、“金卡”和“金税”为代表的重大信息化应用工程；1997 年，召开了全国信息化工作会议；党的十五届五中全会把信息化提到了国家战略的高度；党的十六大进一步作出了以信息化带动工业化、以工业化促进信息化、走新型工业化道路的战略部署；党的十六届五中全会再一次强调，推进国民经济和社会信息化，加快转变经济增长方式；十七大报告根据新世纪新阶段的时代要求，为我国信息化发展赋予了新的重任，将信息化作为与工业化、城镇化、市场化、国际化并举

的重大形势和任务。通过《2006-2020 国家信息化发展战略》、《国民经济和社会发展信息化“十一五”规划》等战略规划的实施，我国信息化进程加速，国民经济和社会信息化发展取得一系列重要成果。

1．信息网络成为支撑经济社会发展的重要基础设施

以电信网、互联网和广播电视网为代表的信息网络基础设施是国民经济和社会信息化的基础支撑平台，是经济社会取得迅速发展的重要条件。当前，我国电话用户、网络规模已经位居世界第一。截至 2008 年底，中国网民规模达到 2.98 亿人，较 2007 年增长 41.9%，互联网普及率达到 22.6%，略高于全球平均水平（21.9 %）。继 2008 年 6 月中国网民规模超过美国，成为全球第一之后，中国的互联网普及再次实现飞跃，赶上并超过了全球平均水平。此外，我国的广播电视网络也已基本覆盖了全国的行政村。

2．信息产业成为重要的经济增长点

信息产业是一种知识产业，在国民经济中的产业关联度极高。发展信息产业可以推动整个国民经济的发展和产业结构的升级，同时，信息产业对国民经济的发展具有倍增器和催化剂作用。发展信息产业能够直接或间接地使国民经济的发展成倍增长，产生一系列的综合经济效益。这些效益的总和，构成了信息产业对整个国民经济的扩散效应。扩散效应综合作用的结果，将使国民经济倍增发展。统计显示，到 2007 年底，我国信息产业增加值占全国 GDP 的比重达 7.9%，电子信息产品出口占全国出口额的 37.6%，占全国高技术产品出口额的近 90%，信息产业无疑已成为国民经济的基础产业、支柱产业和先导产业。

3．信息技术在国民经济和社会各领域得到广泛应用

信息技术在经济和社会各领域的广泛应用，极大地提高了劳动效率，降低了能耗和生产成本，减少了环境污染，有力地推动着经济发展和社会进步。大力推广信息技术应用，发挥其渗透和倍增作用，可以培育出众多新兴产业，促进传统产业结构调整和优化升级，有效提高国民经济运行质量。近年来，我国应用信息技术改造传统产业不断取得新的进展，能源、交通运输、冶金、机械和化工等行业的信息化水平逐步提高。传统服务业转型步伐加快，信息服务业蓬勃兴起。电子商务发展势头良好，电子商务环境明显改进，信用体系逐步完善，现代物流体系建设开始起步，电子商务平台建设取得积极进展，企业网上交易日趋活跃。

4．电子政务为政府管理方式带来深刻变革

推行电子政务是国家信息化工作的重点，是深化行政管理体制改革的重要措施，是转变政府职能、提高行政效率、推进政务公开的有效手段。电子政务可以优化政府工作流程，使政府机构设置更为精简合理，从而解决职能交叉、审批过多等问题；电子政务增加了政府的透明度，实现了平等和规范化服务的创新；电子政务极大地提高了政府工作效率和政府决策的科学化、民主化水平，且使政府信息资源利用更充分、更合理；电子政务为政府提供了新的技术资源、技术能力和技术环境，实现了管理方法的创新。在多年的政府信息化建设中，我国各级政务部门努力利用信息技术，扩大信息公开，促进信息资源共享，推进政务协同，提高了行政效率，改善了公共服务，有效推动了政府职能的转变。根据《国家电子政务总体框架》，到 2010 年，我国将使政府门户网站成为政府信息公开的重要渠道，50%以上的行政许可项目能够实现在线处理，电子政务公众认知度和公众满意度进一步提高，有效降低行政成本，提高监管能力和公共服务水平。

5．国防和军队信息化成为当代新军事变革的核心

当代新军事变革是人类文明由工业时代向信息时代转变的产物，是当代国际综合国力竞争在军事领域的反映。其本质是以工业社会向信息社会过渡为主要背景，以信息技术为核心的高技术发展为直接动力，以信息为基因，以信息化建设和“系统集成”为主要手段，把适应打机械化战争的工业时代的机械化军队，建设成适应信息化战争的信息时代的信息化军队。在信息化条件下，信息已经成为现代战争的战略资源，其重要性日益上升，信息力量已

经成为现代军队作战能力的关键因素。争夺制信息权的斗争，将渗透到战争的各个领域，贯穿作战的全过程，直接影响作战的成败。为实现打赢信息化战争的目标，我军加强了国防和军队信息化建设，近年来取得了重要进展，组织实施了一批军事信息系统重点工程，军事信息基础设施建设有了长足进步，主战武器系统信息技术含量不断提高，作战信息保障能力显著增强。

1.1.2 信息化发展对信息安全的需求

随着信息化发展，信息安全事件不断增多，信息安全问题日渐突出。国民经济和社会发展对信息化的高度依赖，使信息安全已经发展成为涉及国民经济和社会发展各个领域，不仅影响公民个人权益，更关乎国家安全、经济发展、公众利益的重大战略问题。党的十六届四中全会，将信息安全作为国家安全的重要组成部分，明确提出要“增强国家安全意识，完善国家安全战略”，并确保“国家的政治安全、经济安全、文化安全和信息安全”。

1．国家安全对信息安全的需求

人类社会疆域的延伸随着科学技术的发展而不断拓展。在工业时代以前，国土疆域是国家赖以生存的基础。20 世纪伊始，主权国家的疆域不但包括了陆域和海域，也首次包括了空域；而当 1957 年第一颗人造卫星上天后，外层空间的疆域与主权的争夺也随之开始。以信息技术为代表的新的生产力革命以来，人类生产和生活方式发生巨大变革，导致国家安全观念发生深刻变化，以领土、领海、领空安全为标志的传统安全观，正在被“信息安全 + 国土安全”的现代安全观所取代，“信息疆域”理念开始出现，并逐渐成为国家安全防御体系的新的着眼点。

全球信息基础设施使传统的国界概念受到了强烈冲击，在这个不以地理国界为界限的虚拟网络世界中，“跨国”交往非常容易，网上活动的法律关系的主体和客体处于不同国家的控制之下，任何团体和个人，不管其肤色、性别和政治、宗教信仰，也不管身处何方，都可以自由进出。因此，以互联网为基础的全球信息基础设施超越了国家主权，正在创造新的社会系统和权力结构。正是这个新的权力结构的出现，为国家安全带来了新的威胁和挑战，使保卫信息疆域成为国家安全的基本任务。

信息疆域改变了由领土、领海、领空构成的国家空间的结构，使得国家主权有了新的内涵，由此产生了国家信息主权的概念。国家信息主权是指国家的网络和信息系统掌握在代表国家利益和民众利益的统治阶级手中，支撑国家信息主权的信息技术、信息产品控制在代表国家意志的机构中。只有这样，才能保证网络和信息网络系统正常运行，而不受他人的干预和制约，才能有效遏制、削弱、反击对代表国家利益和民众利益政治集团不利的虚假信息。强烈的信息主权意识，不仅是保障国家安全的需要，也是国家发展、民族振兴的必要条件，是维护国家和民族的利益，增强民族内聚力和向心力的“粘合剂”。戍守信息疆域，是巩固信息国防的屏障，是主权国家维护信息主权的天经地义的要务。在信息时代，捍卫本国的信息主权是信息国防的基本内容之一。而强大的信息国防力量则是维护信息主权的前提条件。

2．公民个人权益和公众利益对信息安全的需求

除国家安全外，公共利益以及公民个人、法人和其他组织的合法权益也与信息安全息息相关。信息时代，传统犯罪活动借助网络得到了更大的活动空间，网络诈骗、网络赌博、网络传销、网上销售违禁物品、网络传播淫秽色情等网络违法犯罪活动纷纷出现，相比传统犯罪而言，其危害面更广，犯罪行为更加难以追踪。网络攻击与病毒传播日益增多，危害性不断增高，特别是近年来，网络攻击表现出了趋利性和定向性的明显趋势，极大打击了用户对在线电子商务等互联网应用的信心，企业的商业秘密和用户的敏感信息面临严重威胁。垃圾邮件成为信息社会的一大顽疾，在全球范围内泛滥成灾，屡禁不止。以推销商品、金融诈骗以及造谣生事、地下串联等为内容的各类短信继垃圾邮件之后迅速上升，对公民日常生活、经济利益乃至公共秩序、社会稳定带来极大影响。公民隐私权在信息社会受到巨大冲击，网

络造谣诽谤、攻击谩骂等名誉权纠纷日益增多，多媒体和软件下载、网络浏览等互联网应用使知识产权遭到严重侵害。

当前，我国信息安全形势严峻，关系国计民生基础网络和重要信息系统仍比较脆弱，安全风险较大，每次的重大安全事故都为广大用户的生产生活带来极大不便，也为国家安全留下隐患。2009 年 5 月 19 日，由于几家网游私服之间出现恶性竞争，其中一家以网络攻击的手段向为对方解释域名的 DNS 服务器发动拒绝服务攻击，竟然造成广西、江苏、海南、安徽、甘肃和浙江电信宽带用户网络断网的严重网络安全事件。时隔不久，6 月 25 日我国广东省再次发生大规模断网事故，造成很大影响。

近年来，国家计算机网络应急技术处理协调中心（CNCERT）的技术监测发现，我国境内的网络安全事件持续增加。其中，垃圾邮件事件和网页恶意代码事件增长较快，网页恶意代码每年同比增长近一倍；网页篡改事件特别是我国大陆地区政府网页被篡改事件呈现大幅增长趋势。另据监测，目前病毒、蠕虫、木马、间谍软件等恶意软件仍泛滥成灾。据某安全企业发布的《2008 年中国大陆地区电脑病毒疫情&互联网安全报告》统计，我国 2008 年的病毒数量比 2007 年增长 12 倍以上，全国约有 8100 多万台电脑曾被病毒感染，其中“网页挂马”所传播的木马、后门等恶意程序占据 90%以上。这些恶意软件多以窃取银行帐号、口令和个人信息，获得经济利益为目的，成为当前黑客攻击的重要工具。与此同时，制造木马、传播木马、盗窃账户信息，以及第三方平台销赃、洗钱的巨大黑色产业链已经形成，广大网络用户的利益受到严重侵害。

1.2 信息安全的基本属性

作为一门崭新的学科，信息安全的内涵十分丰富，外延不断扩展，不同的人会对信息安全仍有着不同的认识。但是，从信息的安全获取、处理和使用这一本质要求出发，人们对信息有着三种最基本的安全需求：保密性、完整性和可用性，这是信息安全最基本的追求，也是理解信息安全时的最基本出发点。

1.2.1 保密性

保密性（Confidentiality）这是一个古已有之的需要，有时也被称为“机密性”。在传统信息环境中，普通人通过邮政系统发信件时，为了个人隐私要装上信封。可是到了信息化时代，信息在网上传播时，如果没有这个“信封”，那么所有的信息都是“明信片”，不再有秘密可言。这便是信息安全中的保密性需求。概括说，保密性是指信息不被泄露给非授权的用户、实体或过程，或被其利用的特性。

常用的保密技术包括：防侦收（使对手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（使用密码技术对信息进行加密处理。即使对手得到了加密后的信息也会因为没有密钥而无法读懂信息）、物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露）、信息隐形（将信息嵌入其它客体中，隐藏信息的存在）等。

需要指出，保密性不但包括信息内容的保密，还包括信息状态的保密。例如，在军事战争中，即使无法破解对方的加密信息，但仍可从敌方通信流量的骤增情况上推断出某些重要的结论（例如可以推知敌方将有重大军事行动）。确保通信流保密的技术也有很多，例如可以在保证带宽的前提下通过加入大量冗余通信流，从而保持通信流状态的恒定，避免泄密。

保密性往往在信息通信过程中得到相当程度的重视，然而，信息存储与处理中的安全信息保密问题在当前相当突出，常被人们所忽视。

1.2.2 完整性

完整性（Integrality）是指信息未经授权不能进行更改的特性。即信息在存储或传输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特性。

完整性与保密性不同，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。影响信息完整性的主要因素有：设备故障、误码、人为攻击、计算机病毒等。

保护信息完整性的主要方法有：协议（通过各种安全协议来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）、检错和纠错编码方法（通过设计编码方案，完成检错和纠错功能）、密码校验和方法（对信息进行数学运算后形成信息摘要，一旦信息发生改变，信息的摘要也随之改变）、公证（请求管理或中介机构证明信息的真实性）。

1.2.3 可用性

可用性（Availability）是信息可被授权实体访问并按需求使用的特性。例如，在授权用户或实体需要信息服务时，信息服务应该可以使用，或者是信息系统部分受损或需要降级使用时，仍能为授权用户提供有效服务。可用性一般以系统正常使用时间与整个工作时间之比来度量。

信息的可用性与硬件可用性、软件可用性、人员可用性、环境可用性等方面有关。硬件可用性最为直观和常见。软件可用性是指在规定的时间内，程序成功运行的概率。人员可用性是指人员成功地完成工作或任务的概率。人员可用性在整个系统可用性中扮演着重要角色，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用性的重要保障。环境可用性是指在规定的环境内，保证信息处理设备成功运行的概率，这里的环境主要是指自然环境和电磁环境。

1.3 信息安全概念的演变

什么是信息安全？怎样理解信息安全？这是信息安全理论研究和实践工作中的基本问题。自有人类以来，信息交流便成为一种最基本的人类社会行为，是人类其它社会活动的基础，自然会出现对信息交流的各种质量属性的期望。例如在面对面的交流中，我们就可能关心，对方的话是不是真的，对方的话我是否听清楚了，我们之间的谈话是否被人听到了。因此，对信息安全的需求一直是普遍存在的，在军事斗争中更上升为决定战争成败的重要因素，其根本目的是确保军事指令不被敌人知悉，同时确保没有被改动过，即确保信息的保密性以及完整性。现代信息技术革命以来，政治、经济、军事和社会生活中对信息安全的需求日益增加，信息安全作为有着特定内涵的信息科学门类逐渐得到重视，其概念不断演变。

1.3.1 通信保密

几千年的时间里，军事领域对信息安全的需求使古典密码学得到诞生和发展。到了现代，信息安全首先进入了通信保密（COMSEC）阶段。通信保密阶段的开始时间约为 20 世纪 40 年代，其时代标志是 1949 年 Shannon 发表的《保密系统的信息理论》，该理论将密码学的研究纳入了科学的轨道。在这个阶段所面临的主要安全威胁是搭线窃听和密码学分析，其主要的防护措施是数据加密。

在该阶段人们关心的只是通信安全，而且主要关心对象是军方和政府。需要解决的问题是在远程通信中拒绝非授权用户的信息访问以及确保通信的真实性，包括：加密、传输保密、发射保密以及通信设备的物理安全，通信保密阶段的技术重点是通过密码技术解决通信保密问题，保证数据的保密性和完整性。当时涉及的安全性有：保密性，保证信息不泄露给未经授权的人或设备；可靠性，确保信道、消息源、发信人的真实性以及核对信息接收者的合法性。图 1-1 展示了通信保密时代关心的主要安全威胁。

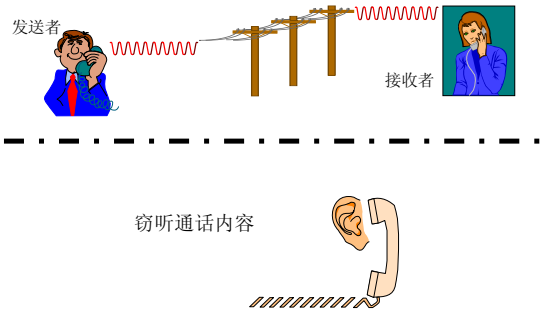


图 1-1　通信保密时代关心的主要安全威胁

1.3.2　计算机安全和信息系统安全

进入 20 世纪 70 年代，通信保密阶段转变到计算机安全（COMPUSEC）阶段，这一时代的标志是 1977 年美国国家标准局（NBS）公布的《数据加密标准》（DES）和 1985 年美国国防部（DoD）公布的《可信计算机系统评估准则》（TCSEC），这些标准的提出意味着解决信息系统保密性问题的研究和应用迈上了历史的新台阶。

进入 20 世纪 80 年代后，计算机的性能得到了成百上千倍的提高，应用的范围也在不断扩大，计算机已遍及世界各个角落。而且人们正努力利用通信网络把孤立的单机系统连接起来，相互通信和共享资源。但是，随之而来并日益严峻的问题是计算机中信息的安全问题。由于计算机中信息有共享和易于扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、伪造和破坏。因此人们开始关注计算机系统中的硬件、软件及在处理、存储、传输信息中的保密性。主要手段是通过访问控制，防止对计算机中信息的非授权访问，从而保护信息的保密性。但是，随着计算机病毒、计算机软件 Bug 等问题的不断显现，保密性已经不足以满足人们对计算机安全的需求，完整性和可用性等新的计算机安全需求于是开始走上舞台。图 1-2 列举了计算机安全时代关心的若干安全威胁。

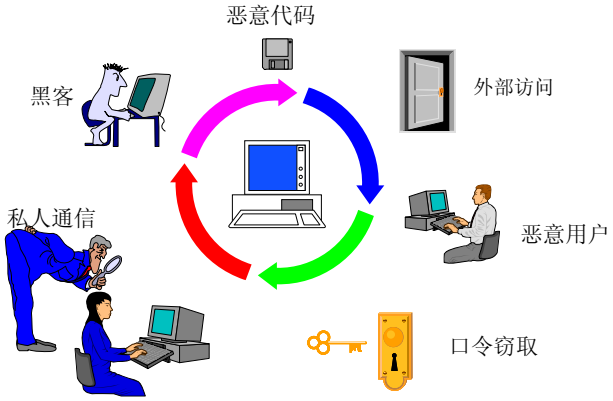


图 1-2　计算机安全时代关心的若干安全威胁

进入 20 世纪 90 年代之后，信息系统安全（INFOSEC）开始成为信息安全的核心内容。此时，通信和计算机技术已经相互依存，计算机网络发展成为全天候、通全球、个人化、智能化的信息高速公路，互联网成了寻常百姓可及的家用技术平台，安全的需求不断地向社会的各个领域扩展，人们的关注对象从计算机转向更具本质性的信息本身，继而关注信息系统的安全。人们需要保护信息在存储、处理或传输过程中不被非法访问或更改，确保对合法用户的服务（即防止出现拒绝服务）并限制非授权用户的服务，确保信息系统的业务功能能够正常运行。在这一阶段，除了保密性、完整性和可用性之外，人们还关注不可否认性需求，即信息的发送和接收者事后都不能否认发送和接收的行为。

1.3.3 信息保障

20 世纪 90 年代末，对于信息系统的攻击日趋频繁，安全不再满足于简单的防护，人们期望的是对整个信息和信息系统的保护和防御，包括对信息的保护、检测、反应和恢复能力。同时，安全与应用的结合更加紧密，其相对性、动态性等特性日趋引起注意，追求适度风险的信息安全成为共识，安全不再单纯以功能或机制的强度作为评判指标，而是结合了应用环境和应用需求，强调安全是一种信心的度量，使信息系统的使用者确信其预期的安全目标已获满足。

为此，美国军方率先提出了信息保障（IA）的概念：“保护和防御信息及信息系统，确保其可用性、完整性、保密性、鉴别、不可否认性等特性。这包括在信息系统中融入保护、检测、反应功能，并提供信息系统的恢复功能。”

信息保障除强调了信息安全的保护能力外，还提出要重视提高系统的入侵检测能力、系统的事件反应能力以及系统在遭到入侵引起破坏后的快速恢复能力。它关注的是信息系统整个生命周期的防御和恢复。这样一个由保护、检测、反应、恢复等内容构成的框架如图 1-3 所示。

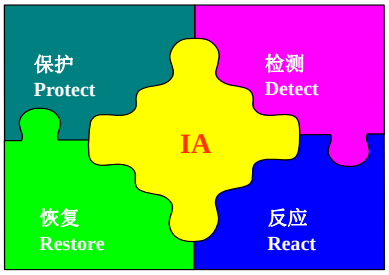


图 1-3　信息保障的四大功能

近年来，美军围绕信息保障发布了多项法令和技术指南。《信息保障技术框架》（IATF）确立了“纵深防御”的技术思路，并指出其适用于任何组织的任何信息系统或网络。8500.1 号和 8500.2 号国防部令则分别确立了美军信息保障的政策框架和技术实施要求。

“信息保障”是信息技术发展到今天，美军为确保复杂战场环境中信息和信息系统的安全而提出的概念，代表了美军对信息安全发展阶段的最新认识。这个概念同时也适用于民用信息系统。就目前来说，虽然美国的军民信息安全合作很多，但“信息保障”仍具有很强的军事色彩。

此外，近年来许多的国家和组织也为信息安全作了不同定义，这些定义的侧重点虽然各有不同，但就技术性而言，多将信息安全归结为信息和信息系统的保密性、完整性和可用性需求。例如美国在 2002 年《联邦信息安全管理法案》（FISMA）中提出：“术语‘信息安全’指保护信息和信息系统，防止未经授权的访问、使用、泄露、中断、修改或破坏，以提供：（A）完整性，防止对信息进行不适当的修改或破坏，包括确保信息的不可否认性和真实性；（B）保密性，信息的访问和披露要经过授权，包括保护个人隐私和专有信息的手段；以及（C）可用性，确保可以及时可靠地访问和使用信息。”

1.3.4 新的信息安全观

信息安全的极端重要性正在引起各国的高度关注，发达国家普遍视信息安全为国家安全的基石，将其上升到国家安全的高度去认识和对待。在这样一个战略高度上，信息安全概念有了更广阔的外延，仅仅从保密性、完整性和可用性等技术角度去理解信息安全已经远远不够了，在世界范围内，新的信息安全观正在逐渐形成。

与传统的信息安全概念不同，新的信息安全观体现在看待信息安全问题的角度已从关注简单的技术后果扩展为关注信息安全对国家政治、经济、文化、军事等全方位的影响。之所以强调与传统信息安全概念的不同，是因为这种影响有时并非源于网络与信息系统自身发生

的安全问题，而在于信息技术的应用方式和信息内容的传播对国家和社会的运行乃至大众的心理活动及其行为所产生的潜移默化的重塑作用。就其作用途径而言，既包括传统的网络与信息系统，也包括信息内容本身。

这里以信息安全与文化安全的关系为示例进一步阐释这一问题。国家文化安全是一个与文化扩张和文化霸权相对应的概念，涉及意识形态和民族文化两个方面。意识形态与国家政权结合在一起，靠国家政权来维护与传播，意识形态的危机必然导致政权危机。而民族文化及其认同则是国家认同的基础以及维系民族和国家的重要纽带，也是国民凝聚力之所在。如果民族文化受到挑战或者质疑，则民族认同的范畴就会出现危机，随之而来的民族凝聚力的涣散不仅是一个民族衰微败落的征兆，更孕育着国家危机。互联网本身是文化的载体和传播渠道，其快速发展使西方文化入侵获得了前所未有的机会。例如，进口的信息技术产品特别是娱乐、休闲产品已经成为西方文化入侵的排头兵，不断向年轻一代灌输着西方的意识形态、生活方式和价值理念。当前，互联网上的信息资源主要集中于英语环境，非英语环境的信息内容远远无法与之抗衡。事实上，信息资源之间的差距会形成国家和民族竞争力上的差距。当许多国家正在考虑如何抵制美式文化入侵的时候，以英语环境为基础的互联网社会又使得如何保护和发扬本民族文化的问题显得更加紧迫。西方很多国家对信息时代的文化入侵极为警惕。例如欧洲大陆一向将美国好莱坞电影视为一种对自身的文化入侵，并敬而远之。2005 年以来，谷歌（Google）的数字图书馆计划又引起了欧洲人的忧虑。根据谷歌在 2004 年 12 月首次公布的数字图书馆计划，将扫描牛津、哈佛、斯坦福和密歇根等四所大学以及纽约公共图书馆的数百万本图书，并把它们放到网上。欧洲人视此为变相的美国文化入侵，担心欧洲大陆对人类历史的贡献会被谷歌抹杀，以美国为中心的英美文化将会垄断整个世界。

显然，上述问题是随着信息化发展而逐渐产生的，其既不同于传统的信息保密性、完整性、可用性等技术概念，且后果也超越了对信息和信息系统的影响，而这些问题的解决，也需要综合考虑到政治、经济、文化等因素。

因此，在新的信息化发展形势下，可以这样理解信息安全的概念：信息安全是要保障信息化健康发展，防止信息化发展过程中出现的各种消极和不利因素，这些消极和不利因素不仅仅表现为信息被非授权窃取、修改、删除以及信息系统被非授权中断（其核心仍是信息的保密性、完整性和可用性），还更深刻地表现为对国家安全、公众利益和个人权益的影响。这种影响可能来源于计算机、网络或系统的技术原因，也可能来源于信息内容本身。

进入 21 世纪后，信息技术以及信息安全相关问题日益成为国与国的政治和经济交往中的重要议题，成为很多国家决策外交事务时的关键考虑因素。联合国意识到了为推进全球信息社会建设而就信息安全概念达成国际共识的必要性，1998 年以来的每届联合国大会上均专门商讨信息安全的概念及信息安全的主要威胁。1999 年，俄罗斯向联合国提交了《从国际安全的角度来看信息和电信领域的发展》的报告，旗帜鲜明地将信息安全定义为保护个人、社会和国家在信息领域的根本利益，尤其将无节制的跨界散布信息、操纵信息流动、破坏社会心理和精神环境等列为主要的信息安全威胁之一。显然，这一概念从根本上挑战了西方一些国家利用信息优势影响他国意识形态、从而达到其政治目的的正当性，因此一度受到西方国家强烈抵制。但近年来，越来越多的国家普遍认识到，对信息的传播进行有效管理是维护国家利益的重要前提。2006 年 10 月 20 日，俄罗斯联合中国等国继续向联合国提交了《从国际安全的角度来看信息和电信领域的发展》的决议草案，该草案最终以 169 票对 1 票获得通过，唯一投反对票的国家是美国。这标志着国际社会对当前信息安全的基本概念初步达成共识，联合国也同时呼吁各国继续就信息安全的有关概念和对信息安全的一般看法向秘书长通告意见。

1.4 信息安全的非传统安全特点

信息时代，信息安全已经成为国家安全的重要组成部分。但与国家安全领域的很多传统安全因素不同，信息安全具有典型的非传统安全特征。在全社会普及信息技术的情况下，信息安全威胁来源呈现出多元化的趋势；信息系统的复杂性、信息技术广泛的渗透性使信息安全的攻击极易得逞，成本可以极低，但防御却难上加难，攻击和防范具有完全的不对称性；关键基础设施的互依赖性、网络的互联互通带来了信息安全事件的全球“即时效应”和“连锁效应”，使得信息安全事件影响广泛，控制难度加大；信息技术的渗透作用和对国家与社会运行的支撑作用，决定了信息安全事件的后果可能极其严重，上至国家安全，下至公民个人权益，均无从幸免；传统安全威胁从发生、发展直至造成后果，往往需要相对较长的时间，即使战争中的“闪电攻击”也不可能突破时间和空间的物理限制，而信息安全事件却可以没有任何征兆，不需要攻击者在物理上接近攻击目标，更不需要耗费可被对方感知的大量时间，倏忽之间便已“攻城掠地，得胜回朝”，这种突发性为安全预警和响应带来了巨大挑战；攻击的便利性和可能的巨大获利，使传统安全威胁没有理由不倾向于使用信息技术手段来达到危害他国安全的目的，信息战甚至成为未来战争的基本形式，信息安全与传统安全因素之间显现出高度的伴随性。

1.4.1 威胁的多元性

传统安全环境下，国家安全威胁的构成相对简单，普通人即使有挑战国家政权和危害国家安全的强烈动机，也基本上不具备成功的途径和工具。但在信息时代，展现在我们面前的则是一种全新的国家安全威胁范式。这种威胁范式的首要特征，就是安全威胁呈现多元化趋势。

就现代信息技术发展水平而言，网络与信息系统越复杂，各种安全漏洞存在的可能性就越高，安全管理的难度也越大，与此相对的，则是攻击网络与信息系统的工具和方法愈加简单和智能化。无论国家、团体出于政治、经济目的还是仅仅因为个人泄愤、炫耀，都可以在此“一试身手”，花样翻新，途经多样，任何一种危害均不容忽视。而目前各国的法律和技术手段对很多攻击行为特别是跨国攻击的威慑力还远远不够，很多行为都得不到有力追究，更加剧了各类威胁主体活动的频繁性。

2000 年，美国发布了《信息系统保护国家计划》，对信息时代的威胁作了如下战略判断：“我们面临着很多危险。……在惹是生非的黑客、硬件和软件缺陷、计算机犯罪以及更令人担忧的敌对国家和恐怖分子的处心积虑的攻击面前，我们实在是脆弱不堪。”“美国的对手分布广泛。从 20 世纪 70 年代开始，我们就了解到一个沉痛的事实：我们的某些敌人有时是非国家组织，包括恐怖分子、毒品贩子和国际罪犯。他们对美国的政策、目标和价值观念持反对态度并且不以外交方针和军事对抗的形式来表现。针对美国基础设施进行成功的计算机攻击是他们采用的一种不错的方法，而且很适合他们的口味和目的。”

威胁的多元性意味着，防御者很难搞清进攻是来自国内还是国外，也很难确切地知道某次攻击是一般的犯罪活动，还是战争的前奏。一个弱国，可以收买个人或犯罪团伙对强国发起信息攻击，可被攻击者却很可能面临找不到主使者的窘境。

此外，面对自然威胁，网络与信息系统同样体现出了严重的脆弱性，洪水、飓风、地震、火灾甚至普通的天气变化，都可能引起电力中断、电缆破坏、计算机元器件受损等事故，从而导致大面积信息安全事件。

1.4.2 攻防的非对称性

自 20 世纪初开始，摧毁或破坏为军事力量提供支持的通信、供给和经济基础设施便成为一条重要的军事原则，被认为同攻击军事力量几乎同等重要，这是各国大力保护关键基础设施的根本原因。传统上，各国的关键基础设施一般处于对手能够作用到的物理范围之外，

而信息时代的到来则为其潜在对手提供了全新的选择，使其基础设施正处在若干年前看起来还遥不可及的攻击方式的危险之中。导致这一情况出现的根本原因，是信息安全攻击与防御的非对称性。

1．攻防技术非对称

信息技术属于高科技技术，但大量自动化攻击工具的出现，已经使得入侵网络与信息系统的门槛降到极低。操作系统、应用软件不可避免地存在大量漏洞，这些漏洞信息完全是公开的。虽然根据业界的规则，在补丁程序发布之前，漏洞信息不会事先公布于众，但由于很多网络与信息系统疏于及时更新补丁程序，导致这些网络与系统存在巨大的安全脆弱性。网络的全球互联特点，使这些安全脆弱性完全对全球开放。针对已知的系统漏洞以及用户的一些不良使用习惯（例如随意下载来历不明的软件、口令过于简单等），攻击者们开发了很多强有力的攻击工具，并通过互联网广泛传播。这些工具使用方便，且往往伴有详细的攻击教程，甚至只掌握初级计算机应用水平的人，都可以依靠这些工具完成复杂的攻击行动。对于某些功能特别强大的攻击软件，则有人明码标价公开出售。甚至有攻击者在使用木马程序控制别人计算机后（受害主机俗称“肉鸡”）出售对计算机的控制权。

2．攻防成本非对称

攻防技术的非对称带来了攻防成本的非对称。一台计算机、一条网线就可以组成作案工具，一个普通的黑客顷刻间就能将许多人花费大量人财物力建设起来的网络系统失效，犯罪成本极低。例如在互联网上的攻击工具广告中，一个拒绝服务（DDoS）攻击软件为 1500 元，除去计算机等一次性购置成本和微不足道的网络资费外，这几乎是一个攻击者所需要花费的全部成本，但 DDoS 造成的破坏则可以使一个电子商务网站在数天之内损失几百乃至几千万元的营业额。

除技术成本低廉外，网络攻击具有很好的隐蔽性，攻击者的风险成本也极低。不同于攻击物理设施，对网络与信息系统的攻击不需要物理上接近。攻击可以来于自世界上任何地方，跨越多个通信网络，可以有效掩盖其身份和位置，而追踪这些攻击却非常困难且耗时极多。就目前技术水平而言，还缺乏针对网络攻击卓有成效的反击和追踪手段。一些经验丰富的攻击者往往通过控制“宿主机”实行远程甚至跨国作案，打击难度很大。

对国家安全而言，攻防成本的非对称性有着特殊的意义。一些势力弱小的国家和政治团体很难承受军事进攻的巨额成本，但借助网络攻击，这些国家和团体获得了极大的攻击机会。他们不用劳师远伐，不用兴师动众，不费一枪一弹，就可以轻易撕破对手依靠传统国防力量构筑的国家安全屏障。

3．攻防主体非对称

传统安全概念中，战争是政治集团特别是国家之间发生的相当长时间、相当大规模的一种冲突，攻防双方一般具有相当的实力，很少有国家去愚蠢地选择“鸡蛋碰石头”，试图向实力远远超出自己的对手挑战。但非传统安全形势下，弱小一方与超级大国之间的实力差得到了大大弥补甚至消除，完全不同量级的选手站到了同一擂台上，而胜负的天平也不再总是偏向强者一边。不但弱国、政治团体可以向强大的国家发起攻击，甚至个人也拥有了挑战国家的机会。

1.4.3 影响的广泛性

所谓信息安全事件，是指由于自然灾害、设备软硬件故障、人为失误或破坏等原因严重影响到网络与信息系统的正常运行，出现业务中断、系统和数据破坏、信息泄密等，或出现违法和有害信息，从而对国家安全、公共利益以及公民个人权益造成不良影响以及造成一定程度直接和间接经济损失的事件。虽然网络与信息系统的安全防护逐渐增强，公众的信息安全意识不断提高，但不论从国际还是国内看，信息安全事件仍逐年上升，影响极为广泛，很容易由局部事件演变成全局事件，且在演变过程中不断放大。

1．影响人群十分广泛

信息化的发展，改变了人们的生活和工作方式，通过网络获取信息、办理事务、在线购物、即时通信等已经成为人们生活和工作的一部分。一旦出现信息安全事件，受影响的人群将极为广泛。

2006 年 12 月 26 日 20 时 26 分和 34 分，我国南海海域发生 7.2、6.7 级地震。受强烈地震影响，中美海缆、亚太 1 号、亚太 2 号海缆、FLAG 海缆、亚欧海缆、FNAL 海缆等多条国际海底通信光缆发生中断，中断点在台湾以南 15 公里的海域，造成国际港澳台通信线路大量中断，互联网访问质量受到严重影响。

由于海底光缆修复困难，这次大规模事故持续了很长时间，导致大批网民受到影响。包括 Youtube、MySpace、Amazon 等在内的美国网站大都不能访问；.COM 等国际域名不能正常注册，域名注册机构无法受理国际域名的注册、续费、信息修改等；中国赴美留学办理工作大面积瘫痪；国内部分电子客票预订网站不能正常使用，特别是国外用户短时不能登录这些网站预订电子客票；国内部分国际外盘交易平台完全瘫痪，国内投资者接收不到数据，也不可以进行下单；很多国外杀毒软件在中国内地没有升级服务器，使得数百万国内个人用户、数十万企业和政府局域网用户无法升级病毒代码库；由于微软的 MSN 服务器位于国外，1500 万 MSN 用户难以正常登录，一些通过 MSN 对外联络的公司无法与客户联系，失去宝贵的商业机遇，一些重要文件也都被“困”在 MSN 邮箱里。

2．扩散性极强

全球联网的互联网，为信息安全事件迅速扩散提供了条件。除非将互联网这一代表了最新生产力发展方向的人类重要发明拒之门外，选择落后的发展方式，否则很难“独善其身”。

当 1988 年时年 23 岁的麻省理工学院学生莫里斯将后来被命名为“莫里斯蠕虫”发布到了当时还处于萌芽状态的互联网上时，这个虽然只有 90 行代码的蠕虫在短短的 2 小时内使世界上 10%的联网计算机瘫痪。但这些计算机的总数也不过 6000 台而已。19 年前的互联网是一个封闭系统，只供科研和军事机构使用，而如今它已向公众开放，信息安全事件的影响已经不可同日而语。

2001 年的 Nimda 蠕虫病毒在短短 24 小时内即感染了超过 220 万台的计算机，并导致约 5 亿美元以上的损失。到了 2003 年，SQL Slammer 蠕虫在短短 5 天内就造成全球 10 亿美元的损失。而 2003 年 8 月的 Sobig 蠕虫则被视为当时传播最迅速的蠕虫，据 ZDNET 报导，仅仅在 1 天之内，美国在线（AOL）就收到高达 1150 万封携带 Sobig.F 的电子邮件。

3．连锁反应突出

1963 年气象学家洛伦兹提出的“蝴蝶效应”正在社会生活各个领域广为验证：一只南美洲亚马逊河流域热带雨林中的蝴蝶，偶尔扇动几下翅膀，可能在两周后引起美国得克萨斯的一场龙卷风。其原因在于，事物具有普遍联系性，任何一样事物产生任何的改变，都会对世界万物产生或多或少的影响。在信息时代，“蝴蝶效应”带来的连锁反应后果是导致信息安全事件影响广泛的另一重要原因。由于各类基础设施之间有着极强的互依赖性，“多米诺骨牌”式的连锁效应会使信息安全事件迅速升级。对一个局部系统甚至区区一个点的攻击最终可能造成国家范围内的大规模基础设施灾难，而攻击者所做的可能仅仅只是推倒了第一块微小的多米诺骨牌而已。

1.4.4 后果的严重性

国民经济和社会发展对信息技术的高度依赖是信息时代的重要特征，也是信息安全极端重要的根本原因。所有经济部门的正常运行，包括能源（电力、石油、天然气）、运输（铁路、航空）、金融、通信等都以网络与信息系统的安全保障为基本条件，世界上大多数国家都已经全面建立在网络与信息系统的支持之上，信息安全事件动辄影响社稷安危，关系全民福祉。

1．推翻国家政权

信息战是信息安全关系国家安全的最直接形式。1991 年的海湾战争，被各国军方认为是第一次把信息战从研究报告中搬上了实战战场。在这场战争中，美国特工利用伊拉克购置的用于防空系统的打印机途经安曼的机会，将一套带有病毒的芯片换装到这批打印机中，并在美军空袭伊拉克的“沙漠风暴”行动开始后，用无线遥控装置激活潜伏的病毒，致使伊拉克的防空系统陷入瘫痪。2003 年的伊拉克战争开始之时，美军就以电子邮件方式向伊拉克军事和民事官员发起攻心战，劝告他们不要再支持萨达姆·侯赛因，同时要求他们提供有关伊拉克大规模杀伤性武器的情报，并且劝他们不要使用生化武器。在当时的伊拉克，互联网还是稀有事物，仅有一少部人可以接触到它，美国相信能够收看电子邮件的人都是伊拉克的精英分子，以此方式来瓦解他们的斗志。

除信息战之外，网上意识形态渗透与反渗透、窃密与反窃密的斗争也十分激烈，特别是在当今时代大规模军事对抗逐渐减少的形势下，网上成为维护国家安全的主战场，信息安全始终是决定政权生死存亡的大事。

2．瘫痪国家基础设施

网络与信息系统在国民经济和社会发展中的基础性、全局性作用正日益增强，保护国家关键基础所依赖的基础信息网络和重要信息系统的安全是国家经济稳定运行的关键。除此之外，国家关键基础设施还是信息战中敌方的重点攻击目标，攻击后果极其严重。虽然根据国际惯例，战争中禁止攻击平民和民用目标，但每一个积极发展信息战能力的国家，都不可能无视攻击电力、金融、交通等民用基础设施的信息系统对战争可能产生的决定性影响，都不可能不将打击对手的经济命脉作为战争迅速取胜的关键。

3．造成巨大经济损失

早在 2000 年，美国商业杂志《信息周刊》公布的一项调查报告曾报道说，计算机病毒和黑客攻击在该年将使全球公司蒙受 15 万亿美元以上的经济损失。报告说，北美地区计算机系统有 3.24%在 2000 年发生过停工，全球这一比例为 3.28%。在被调查的大约 5 万家大企业中，据统计因病毒和攻击所受的损失估计将达 2660 亿美元，相当于美国国内生产总值的 2.5%，如果把众多的中小企业计算在内，病毒和黑客入侵造成的损失还要大得多。

上述统计数据仅仅是世纪之交作出的。进入 21 世纪之后，仅冲击波蠕虫和 SoBig.F 电子邮件型病毒等恶意代码就给全球经济造成了 130 亿美元的损失。美国商务部则表示软件缺陷一年给美国造成的经济损失有 596 亿美元，其中包括因软件漏洞受到的攻击损失。据美国联邦调查局《2005 年计算机犯罪调查》报告显示，仅身份欺诈一项每年给美国造成的损失便达到 526 亿美元。

黑客攻击对中国企业造成的经济损失也在逐年上升。2007 年 4 月开始，一股黑客攻击狂潮席卷国内多家大型网络游戏公司，造成的经济损失达到上千万元。该案后被北京海淀警方成功破获。令人咋舌的是，犯罪嫌疑人仅有区区数人，其目的竟是为了推销防火墙设备。

4．引发公共安全灾难

与病毒和黑客攻击动辄造成数十亿美元经济损失相比，有时基础设施所依赖的各类重要信息系统被攻击后引发的公共安全灾难更为可怕。

2000 年，澳大利亚人威泰克·波顿攻击了该国昆士兰州马鲁奇郡的污水管理系统，致使数百万升未经处理的污水倾泻到当地的公园和河流中，甚至还流淌到附近的酒店里。据澳大利亚环保局的工作人员称，恶意攻击导致水生动物大量死亡，河流散发阵阵臭气，令当地居民无法忍受。该名黑客后被判刑 2 年，据悉他曾向污水管理部门求职，但遭到拒绝，因而怀恨在心，伺机报复。当时他在负责安装这套污水管理系统的公司任职，于 2000 年 3 月至 4 月间至少向污水管理系统实施了 46 次攻击，其中前 45 次攻击没有成功，但也一直没有被发现。

以美国著名信息安全专家斯奈尔为代表的一些人认为，信息恐怖主义在现实中并不存在，迄今也只是发生了上述一起造成公共灾难的人为信息安全事件而已。这些观点源于斯奈尔等专家对“信息恐怖主义”理解的不同。事实上，信息安全事件并不都以“将人炸成碎片”为危害公共安全的最极端表现形式。当前越来越多的行业采用数字控制系统（DCS）以及监督控制和数据采集系统（SCADA）来管理和监控各种设备，其中以电力系统为典型代表。DCS/SCADA 系统与互联网和电信网的技术原理完全不同，且安全防护有很多特殊性，例如 DCS/SCADA 系统通常是需要少量供电的小型的独立系统，在其体积和供电量的限制下，很多安全措施很难应用，且这些系统是以实时模式运行的，采用安全措施可能会降低其性能并对整个大的系统的同步造成影响。DCS/SCADA 系统的安全直接决定了很多工业控制系统的运行状况，将污水和净化水的输入方向互换、将城市供热系统的温度值修改为极高或极低，对公共安全以及公众心理造成的后果要远远超过一次常规的恐怖袭击事件。正是这一原因，使美国政府将 DCS/SCADA 安全列为国家信息安全战略的优先对象，其国会也在 2006 年间组织了数次听证会，专门研究安全现状和对策。

1.4.5 事件的突发性

各类信息安全威胁往往具有潜伏性和不可预测性，使得信息安全事件对被攻击一方而言呈现出极强的突发性，被攻击者往往因此丧失了宝贵的防御时间，为信息安全事件处置带来了极大挑战——事实上很多事件最终也没有被发现，损失评估更无从谈起，例如敏感信息的泄密，这则是更加可怕的事情。

信息安全防御及攻击技术极为多样和微妙，用户通常很难知道已经受到攻击以及谁在攻击、怎样攻击。信息安全攻击行为完全发生在网上虚拟世界，源头完全无法在事前判定，攻击后一般不对物理设施造成破坏，攻击行为可以不留痕迹，被攻击者甚至丝毫察觉不倒系统被攻击后的异样。尤其是国家层面的信息战，往往攻击于无形之中，难以发现和防备。一条攻击指令，从发出到到达千里之外的目标计算机，也仅仅是瞬时而已。

由于现代网络与信息系统的复杂度很高，有些事故可能是由于误操作、偶然故障或系统设计错误引起的，如何将有意攻击与偶发故障相区别是件极其困难的事情。近年来，信息安全攻击工具和手段不断进步，其隐藏攻击踪迹的能力越来越高。例如 2005 年以来，Rootkit 已成为众多恶意软件的藏身工具，在其掩护下恶意软件可轻易逃脱反病毒及反间谍软件的监控而不被发觉。有安全公司表示，到 2008 年，上述情况将大肆泛滥，形成前所未有的安全风险。

另外，在长达数年的“攻击准备”过程中，系统完全有可能已经被渗透或损害——攻击者可以在对方软件或硬件中设置“逻辑炸弹”，平时表现完全正常，到关键时刻只需一个特殊指令便会启动。例如，有些军火商在出口的飞机、坦克、军舰、导弹发射架或超级计算机上植入一些暗藏的芯片，在适当的时候启用这些芯片，整个系统便可以被摧毁，而要发现这些芯片，几乎是不可能的事情。

为有效扭转信息安全事件突发性带来的被动局面，目前很多国家都在加大信息安全预警和检测能力。预警的核心目标就是在可能危及网络与信息系统的安全事件发生之前，依据对某些迹象的分析判断，提出其可能造成的危害估计，提前采取防范警告和措施，从而将事件的危害程度控制在网络与信息系统可以接受的范围内。安全检测的目的则是发现系统的漏洞，加强系统安全功能，提高系统安全防护性能和抗破坏能力，为评估已运行系统的安全性能提供依据，并提供有针对性的安全建议。

1.5 我国信息安全保障工作

信息安全的重要性已经使其成为国家安全的战略性问题，必须从总体上把握，不断完善信息安全战略，并将其作为国家安全战略的核心部分。2003 年，中共中央办公厅、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》（中办发[2003]27号），标志着我国信息安全保障工作有了基本纲领和大政方针，指导思想和主要任务得以明确。2003 年以来，按照 27 号文的部署，我国信息安全保障工作进展顺利，信息安全保障水平大为提高。

1.5.1 总体要求

27 号文件确定的我国信息安全保障工作的总体要求是，坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全。

积极防御就是要充分认识信息安全风险和威胁，立足安全防护，加强预警和应急处置，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统；从更深层次和长远考虑，积极防御还包括国家要有一定的信息对抗能力和反制手段，从而对信息网络犯罪和信息恐怖主义等形成威慑。

综合防范就是要从预防、监控、应急处理和打击犯罪等环节，法律、管理、技术、人才等各个方面，采取多种技术和管理措施，通过全社会的共同努力，全面提升信息安全防护能力。

1.5.2 主要原则

27 号文件确定的我国信息安全保障工作的主要原则是，立足国情，以我为主，坚持管理与技术并重；正确处理安全与发展的关系，以安全保发展，在发展中求安全；统筹规划，突出重点，强化基础工作；明确国家、企业、个人的责任和义务，充分发挥各方面的积极性，共同构筑国家信息安全保障体系。

1．立足国情，以我为主

安全单靠花钱是买不来的。发展信息和信息安全高技术、发展国家信息产业和信息安全产业、摆脱关键技术和设备受制于人的被动局面是掌握信息安全主动权的根本出路。必须注重自主创新、自主可控。要大力推广应用国产软件和设备。另一方面，也要处理好自主研发与引进、采用国外先进技术和产品的关系，不能简单地认为只有自己的技术才是安全的，凡是国产的设备就是可控的。要积极开展国际合作，认真学习国外信息和信息安全新技术，合理引进和利用信息安全产品。同时，要加强对引进技术和产品的安全可控研究，努力做到趋利避害，为我所用。

2．坚持管理与技术并重

信息安全保障工作包括技术和管理两个方面，缺一不可。但从目前我国实际发生的安全事件看，有很多事件都是由于管理不到位，责任不落实造成的。因此应建立和完善信息安全管理责任制，加强管理，落实责任。

同时，信息安全是高技术的对抗，从根本上讲，解决信息安全问题还是要通过发展信息安全高技术。要坚持管理与技术并重，积极发展和采用先进技术来解决信息安全问题，同时也要注重通过加强管理弥补技术上的不足。

3．正确处理安全与发展的关系，以安全保发展，在发展中求安全

在信息化规划和建设中，应同步考虑信息安全问题，始终坚持一手抓信息化发展，一手抓信息安全保障工作。没有安全保障的信息化，会严重威胁国家安全和社会稳定，影响公民权益和公众利益。同时，信息安全问题解决不好，有价值的信息不能上网，可以利用网络处理的业务不能用网络来处理，会严重影响和制约信息化的发展。

信息安全是信息化推进中出现的新问题，只能在发展的过程中加以解决。要坚持保障和促进信息化发展这一根本原则。全部通过不上网、不共享、不互联互通来保安全，或者片面强调建专网，这样做的结果只能是造成不必要的重复建设，大量网络资源得不到充分利用，增加了信息化的成本，降低了信息化效益，失去了发展机遇。

4．统筹规划，突出重点，强化基础工作

信息安全保障工作涉及到信息化建设的各个环节，包括法律、管理、技术、人才、意识等各个方面，是一个复杂的系统工程这就要求注重统筹规划、全面防护，从各个层面，各个环节上加强综合性的信息安全保障工作。与此同时，还要突出重点，有所为有所不为，将有限的资源用于基础部分、关键地方、要害部位。要重点防止那些关系到国计民生的基础信息网络和信息系统在遭到攻击、破坏和发生事故时，导致基础服务大面积瘫痪，防止为经济和社会造成巨大损失。

5．充分发挥各方面的积极性，共同构筑国家信息安全保障体系

信息安全保障是国家的大事。政府应着重从政策引导、监督管理、人才培养、增强意识及基础技术研究开发等方面加强信息安全保障工作，同时也要做好政府本身信息系统的安全建设和管理工作，为社会做出榜样。但是，信息安全保障不仅是政府的事，在更大层面上，信息安全保障是广大企业、公民个人的责任和义务，需要全社会的共同努力。

1.5.3 主要基础性工作

按照 27 号文确定的“积极防御、综合防范”的方针，我国有关部门近年来抓紧开展了以下各项基础性工作，取得了明显进展。

1．实行信息安全等级保护

不同的信息系统有着不同的安全需求，必须从实际出发，综合平衡安全成本和风险，优化信息安全资源的配置，确保重点。信息安全等级保护制度是国家信息安全保障工作的基本制度，是国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

为了加快推进信息安全等级保护工作，在多年探索和试点的基础上，公安部、国家保密局、国家密码管理局和原国务院信息化工作办公室于 2007 年 6 月联合发布了《信息安全等级保护管理办法》,《信息系统安全等级保护定级指南》、《信息系统安全等级保护基本要求》等技术标准也已施行。目前，我国信息安全等级保护进入全面实施阶段，全国范围内的信息系统定级工作已经基本完成，等级建设和测评工作即将启动。

2．开展信息安全风险评估

信息安全风险评估是运用科学的方法和手段，系统地分析网络与信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的防护对策和整改措施，并为防范和化解信息安全风险，或者将风险控制在可接受的水平，从而为最大限度地保障网络和信息安全提供科学依据。

为此，27 号文明确提出，要重视信息安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉密程度和面临的信息安全风险等因素，进行相应等级的安全建设和管理。这一要求将开展信息安全风险评估工作作为提高我国信息安全保障水平的一项重要举措。

2006 年 1 月，国务院信息化工作办公室印发了由国家网络与信息安全协调小组讨论通过的《关于开展信息安全风险评估工作的意见》。《意见》要求，信息安全风险评估作为信息安全保障工作的基础性工作和重要环节，应贯穿于网络和信息系统建设运行的全过程。《意见》对我国信息安全风险评估工作做了安排：要从抓试点开始，逐步探索组织实施和管理的经验，用 3 年左右的时间在我国基础信息网络和重要信息系统普遍推行信息安全风险评估工作，全面提高我国信息安全的科学管理水平，提升网络与信息系统安全保障能力，为保障和促进我国信息化发展服务。

3．加强密码技术应用，建设网络信任体系

密码是保障信息安全的核心技术，是网络环境下实现信息保护和安全认证的有效手段。在解决网络信息系统的身份认证、安全接入以及信息的保密性、完整性等方面发挥着特殊的

不可替代的作用，有效地使用密码技术是信息安全保护的关键。当前，随着信息网络的发展，密码应用领域不断拓宽。在为党、政、军各级领导机关提供秘密通信的同时，密码已广泛应用于经济、科技、文化和社会生活的各个领域，成为现代社会的重要战略资源。因此，充分发挥密码在保障国家安全、社会稳定、经济发展和公众利益中的重要作用，促进国家信息化的健康发展成为当今时代的重要课题。

针对面向商用和公众服务的密码需求日益增多这一形势，27 号文要求我国密码管理工作必须适应经济全球化和进一步开放的大环境，按照“满足需求、方便使用、加强管理”的原则，修改完善密码管理法规，建立健全适应信息化发展需要的密码管理体制。

同时，27 号文还要求加强以密码技术为基础的信息保护和网络信任体系建设，建立协调管理机制，规范和加强以身份认证、授权管理、责任认定等为主要内容的网络信任体系建设。截至目前，原信息产业部以及工业和信息化部根据《电子签名法》的授权，先后批准 30 家单位获得了电子认证服务许可。这些机构颁发的数百万张电子证书广泛应用于网上税收、工商管理、社区服务、招标采购、网上银行、企业供应链管理、电子商务平台等领域，为经济发展起到了重要的保驾护航作用。

4．高度重视应急处理工作

在信息安全事件不可能完全杜绝的情况下，信息安全应急处理发挥着重要的作用，是信息安全防护体系中的重要一环。27 号文明确要求，各基础信息网络和重要信息系统建设要充分考虑抗毁性与灾难恢复，制定和不断完善应急处置预案。加强信息安全应急支援队伍建设，鼓励社会力量参与灾难恢复与灾难备份设施建设和提供技术服务，提高信息安全应急响应能力。

近几年，通过政策引导以及有关部门和社会各界的共同努力，国家重要信息系统灾难恢复工作取得了明显进展。各行业、各省市的灾难恢复建设陆续启动，我国的灾难恢复建设正逐步从探讨进入实践阶段。灾难恢复的第三方专业化服务市场正在形成，较好地推动了我国信息系统灾难恢复工作的开展。

2003 年 10 月，我国建立了国家网络与信息安全信息通报中心，工作重点是做好重要敏感期、重大政治活动和重大网络安全事件的信息通报工作。通报中心的成立，标志着我国信息安全信息通报和预警能力有了显著提高。近年来，我国还大力加强基础信息网络和重要信息系统的应急预案制定和应急演练工作，国家层面的应急指挥协调机制也已初步建立。

5．加强技术研发，推进产业发展

信息安全是高技术的对抗，信息安全产业构成了国家信息安全保障体系的物质基础和技术支撑。加强信息安全技术研发，推进信息安全产业发展是决定我国信息安全保障能力的核心要素。27 号文要求采取积极措施，组织和动员各方面力量，加强信息安全关键技术和相关核心技术的研究开发，提高自主创新能力，促进技术转化，加快产业化进程。

近年来，我国通过实施信息安全专题 863 计划和 973 计划等科研项目，加强了对信息安全关键技术的研究，攻克了一批信息安全重大技术难题。特别是在 863 计划等国家计划的支持下，已经在 PKI/CA 技术、密码标准和芯片、网络积极防御、网络入侵检测与快速响应、网络不良内容监控与处置等方面取得了较大进展。

另外，“十五”期间还组建了多个国家级信息安全研究中心，研究实力不断增强。“十五”计划信息安全专项的实施，已经开始发挥重要作用。我国建立了上海、四川、湖北三大信息安全成果产业化基地，积极开展了信息安全应用示范工程，为国家网络与信息安全技术发展及产业化奠定了基础。

为进一步规范信息安全产品测评认证，为产业发展创造良好的市场环境，2004 年 10 月，国家认监委、公安部等八部委联合发布了《关于建立国家信息安全产品认证认可体系的通知》，要求建立国家信息安全产品认证认可体系。按照这一文件的部署，信息安全产品认证

工作已经进入实施阶段并取得重大进展，信息安全产品强制性认证制度将于 2010 年 5 月 1 日起在政府采购法规定的范围内强制实施。

6．加强法制建设和标准化建设

面对信息化迅速推进过程中出现的一些新问题、新情况，目前各有关部门正在清理、调整和修订现有信息安全法律、行政法规和部门规章。按照 27 号文提出的“抓紧研究起草《信息安全法》，建立和完善信息安全法律制度，明确社会各方面保障信息安全的责任和义务”的要求，几年来有关部门一直在组织起草《信息安全条例》，旨在确立信息安全的基础法律框架。与此同时，有关政府信息公开、信息网络传播权保护的行政法规已经发布，《刑法》修正案完善了对计算机犯罪罪名的规定，保密法修正案正在接收全国人大常委会审议。

为加强信息安全标准化建设，我国在 2002 年成立了全国信息安全标准化技术委员会，抓紧制定了一批急需的信息安全管理和技术标准，逐步建立与国际标准相衔接的中国信息安全标准体系，并大力推进这些标准的贯彻实施。截至目前，我国已制定、颁布 76 项信息安全国家标准，另有 50 项正在制订之中。

7．加快人才培养，增强全民意识

信息安全人才是今后信息安全健康、良性发展的关键。加强信息安全保障工作，必须有一批高素质的信息安全管理和技术人才。为此，27 号文要求加强我国信息安全学科、专业和培训机构建设，加快信息安全人才培养。要采取积极措施，吸引和用好高素质的信息安全管理和技术人才。

根据“加强信息安全人才培养”的要求，近年来我国对信息安全学科建设作了大量投入。2005 年，教育部专门发布《教育部关于进一步加强信息安全学科、专业建设和人才培养工作的意见》（文教高[2005]7 号），从加强信息安全学科体系研究、信息安全硕士点和博士点建设、稳定信息安全本科专业设置、促进交叉学科专业探索多样化培养模式新机制、建立信息安全继续教育制度等十个方面提出了指导性的意见。

2007 年 2 月，为了加强教育部对高等学校信息安全人才培养工作的宏观指导与管理，充分发挥专家学者对信息安全类专业教学改革与建设的研究与指导作用，教育部组建了教育部高等学校信息安全类专业教学指导委员会，使我国的信息安全人才培养工作向前迈进了重要一步。2009 年 3 月，在教育部高等教育司以及工业和信息化部信息安全协调司指导下，教育部高等学校信息安全类专业教学指导委员会启动了全国大学生信息安全竞赛，对增强信息安全专业社会影响、提高广大学生学习热情起到了良好的推动作用。

除人才培养外，全民信息安全意识和技能的提高也是当前我国信息安全工作面临的重要任务。27 号文要求重视对各级领导干部的信息安全教育和法律法规教育，要求开展全社会特别是对青少年的信息安全教育和法律法规教育，增强全民信息安全意识，自觉规范网络行为。为此，各有关部门近年来多次组织大型展览、宣传、主题教育等活动，取得了明显效果。

1.5.4 未来展望

2006 年 3 月 19 日，中共中央办公厅、国务院办公厅印发了《2006-2020 年国家信息化发展战略》（中办发[2006]11 号）。《发展战略》将建设国家信息安全保障体系作为我国信息化发展的重点之一，为今后的信息安全保障工作指明了方向：

“全面加强国家信息安全保障体系建设。坚持积极防御、综合防范，探索和把握信息化与信息安全的内在规律，主动应对信息安全挑战，实现信息化与信息安全协调发展。坚持立足国情，综合平衡安全成本和风险，确保重点，优化信息安全资源配置。建立和完善信息安全等级保护制度，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统。加强密码技术的开发利用。建设网络信任体系。加强信息安全风险评估工作。建设和完善信息安全监控体系，提高对网络安全事件应对和防范能力，防止有害信息传播。高度重视信息安全应急处置工作，健全完善信息安全应急指挥和安全通报制度，不断完善信息安全

应急处置预案。从实际出发，促进资源共享，重视灾难备份建设，增强信息基础设施和重要信息系统的抗毁能力和灾难恢复能力。

大力增强国家信息安全保障能力。积极跟踪、研究和掌握国际信息安全领域的先进理论、前沿技术和发展动态，抓紧开展对信息技术产品漏洞、后门的发现研究，掌握核心安全技术，提高关键设备装备能力，促进我国信息安全技术和产业的自主发展。加快信息安全人才培养，增强国民信息安全意识。不断提高信息安全的法律保障能力、基础支撑能力、网络舆论宣传的驾驭能力和我国在国际信息安全领域的影响力，建立和完善维护国家信息安全的长效机制。”

在贯彻这一战略的过程中，面向新的形势发展提出的新要求，我国信息安全保障工作将在科学发展观的指导下，不断调整发展思路，完善顶层设计，部署实施新的工作，切实服务与国家安全和经济社会全面发展。

本章小结

本章围绕信息化发展与信息安全的关系展开论述，在信息化发展的大背景下重点探讨了信息安全的概念演变。本章的主要内容有：

（1）信息化发展

信息技术已经成为最活跃的生产力要素，成为影响国家综合实力和国际竞争力的关键因素。加快信息化发展，坚持以信息化带动工业化，以工业化促进信息化，这是我国加快实现工业化和现代化的必然选择。

在大力推进信息化的过程中，信息安全问题逐渐突出并成为决定信息化能否健康发展乃至成败的关键因素。上至国家安全，下至公民个人权益和公众利益，都对信息安全提出了极为迫切的需求，信息安全也上升为国家安全的重要组成部分。但信息安全并不是最终的目的，维护信息安全是为了对信息化发展保驾护航，“以安全保发展，在发展中求安全”的信息安全保障工作原则揭示了两者之间的辩证关系。

（2）信息安全概念

虽然信息安全有着很多不同的定义，但从信息的安全获取、处理和使用这一本质要求出发，人们对信息提出了三种最基本的安全需求：保密性、完整性和可用性，这是理解信息安全概念时的起点。随着信息技术的进步及其应用范围的扩大，信息安全的内涵不断丰富，外延不断扩展，传统的信息安全概念也先后经历了通信保密、计算机安全和信息系统安全、信息保障的阶段。

时至今日，传统的信息安全概念已经不足以概括人们对信息安全的需求，在世界范围内，新的信息安全观正在逐渐形成。从信息化发展的本质规律出发，本书提出了新的信息安全观的核心内容。这一新的信息安全观也要求，信息安全问题的解决，除了技术因素外，还需要考虑政治、经济、文化等因素，离不开技术、管理、法律、政策等多种手段的综合运用。当然，作为信息安全专业的本科教材，本书的后续大部分章节还是主要介绍了信息安全的技术对策。

（3）信息安全的非传统安全特点

信息安全有很多特点，对具体特点的阐述依赖于看问题的角度。本章围绕信息安全是一种典型的非传统安全因素这一具有鲜明时代特征的命题，讨论了信息安全的以下特点：威胁的多元性、攻防的非对称性、影响的广泛性、后果的严重性以及事件的突发性。归纳出这些特点，可以使读者增加对信息安全的认识，也通过这些特点进一步阐释了信息安全的重要性。

（4）我国信息安全保障工作

我国对信息安全极为重视，明确了信息安全保障工作的基本纲领和大政方针，包括总体要求和主要原则，并部署了一系列基础性工作。此外，国家信息化发展战略也提出了今后若

干年我国信息安全保障工作的重点。本章之所以介绍这些内容，除了向读者提供更丰富的背景材料外，还希望读者能够从中进一步加深对信息安全特点和规律的把握。

习题

1．举例说明信息化的意义及其对我国的重要影响。
2．解释信息疆域的概念。
3．信息安全的三个基本属性是什么？
4．描述信息安全概念的演变过程。
5．为什么要提出新的信息安全观？新的信息安全观与以前的信息安全概念有什么区别？
6．为什么说信息安全是非传统安全？它有哪些特点？
7．我国信息安全保障工作的总体要求和主要原则分别是什么？
8．我国信息安全保障基础性工作有哪些？
9．我国的国家信息化发展战略对信息安全保障工作提出了哪些要求？

第 2 章　信息安全基础

本章要点

- 信息系统安全要素及其相互关系
- 开放系统互联安全体系结构
- 信息安全保障体系
- “两个中心”支持下的三重信息安全技术保护框架

2.1　信息系统安全要素

以下介绍了影响信息系统安全的主要因素及其相互作用关系。信息安全学科知识体系中有大量崭新的术语和定义，很多术语和定义往往与具体的技术相关。本小节给出的信息系统安全要素涉及到了很多与信息系统安全顶层设计相关的若干重要术语，包括信息安全威胁、脆弱性、风险等。

2.1.1　基础概念

信息系统安全保护的实质是风险管理，信息系统安全保护的直接目的便是控制安全风险。“风险”及其相关概念构成了影响信息系统安全的主要因素，它们不但揭示了信息安全问题产生的原因，也因此导出了信息安全问题的解决方案。

这些基础概念包括：

使命：即一个组织通过信息技术手段实现的工作任务。一个组织的使命对信息系统和信息的依赖程度越高，信息系统安全就越重要。

资产：通过信息化建设积累起来的信息系统、信息、生产或服务能力、人员能力和赢得的信誉等。

资产价值：资产是有价值的，资产价值可通过资产的敏感程度、重要程度和关键程度来表示。

威胁：一个组织的信息资产的安全可能受到的侵害。威胁由多种属性来刻画：威胁的主体（威胁源）、能力、资源、动机、途径、可能性和后果。

脆弱性：信息资产及其安全措施在安全方面的不足和弱点。脆弱性也常常被称为漏洞。

事件：如果威胁主体能够产生威胁，利用资产及其安全措施的脆弱性，那么实际产生危害的情况称之为事件。

风险：由于系统存在的脆弱性，人为或自然的威胁导致安全事件发生的可能性及其造成的影响。它由安全事件发生的可能性及其造成的影响这两种指标来衡量。

残余风险：采取了安全措施，提高了信息安全保障能力后，仍然可能存在的风险。

安全需求：为保证单位的使命能够正常行使，在信息安全保护措施方面提出的要求。

安全措施：对付威胁，减少脆弱性，保护资产，限制意外事件的影响，检测、响应意外事件，促进灾难恢复和打击信息犯罪而实施的各种实践、规程和机制的总称。

在上述概念中，威胁、脆弱性和风险是最核心的概念。

威胁可以宏观地分为自然威胁和人为威胁两大类。自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰、网络设备自然老化等。人为威胁一般又可以分为故意的和非故意的威胁两大类。故意的威胁具有一定的目的、动机和企图。常见的故意威胁有：

带有国家或集团色彩的攻击者，恐怖分子，犯罪分子，黑客（黑客的攻击动机比较复杂，例如获利、炫耀技术等），与外部勾结的内部人员，对自己的单位不满意、怀有报复心理的内部人员，以及潜伏在机构内部的间谍等。非故意威胁没有恶意的目的、动机和企图，但实际上，其造成危害的能力有时甚至超越故意威胁带来的危害。一般而言，这类威胁往往来自于不熟练的系统使用者和维护者。

由威胁源所实施的、导致安全事件发生的行为一般称为攻击。攻击可以分为被动攻击与主动攻击两种类型。被动攻击一般指被动监视通信网络（例如无线电、卫星、微波和公共交换网）上传送的信息，而不对信息的传输、存储和处理过程进行破坏。常见的被动攻击方式如监视明文、解密通信数据、口令嗅探和通信量分析等。主动攻击涉及到对安全机制的破坏和对信息、数据的改动。常见的主动攻击方式如篡改数据、重放、会话拦截、拒绝服务攻击等。

脆弱性是资产本身所存在的，但是如果没有被相应的威胁利用，单纯的脆弱性本身不会对资产造成损害。而如果系统足够强健，即使是严重的威胁也不会导致安全事件发生。即，信息系统的脆弱性是安全风险产生的内因，威胁则是安全风险产生的外因。外因要通过内因起作用，威胁要利用脆弱性才能够造成安全风险。分析脆弱性一般从技术和管理两方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的问题；管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关。

人们的认识能力和实践能力总是有局限性，因此，信息系统存在脆弱性是不可避免的。信息系统的价值及其存在的脆弱性，使信息系统在现实环境中，总要面临各种人为或自然的威胁，存在安全风险也是必然的。信息安全保护的实质，就是在综合考虑成本与效益的前提下，通过安全措施来控制风险，使残余风险降低到可接受的程度，因为如果安全措施的成本超出了实施安全措施、控制风险后可能带来的效益，那么这种安全措施便失去了意义。由于任何信息系统都会有安全风险，人们追求的所谓安全的信息系统，实际是指信息系统在实施了风险评估并做出风险控制后，仍然存在的残余风险可被接受的信息系统。因此，不存在绝对安全的信息系统（即“零”风险的信息系统），也不必要追求绝对安全的信息系统。

2.1.2 各要素间的相互关系

国际标准 ISO/IEC 15408《信息技术 安全技术 信息技术安全评估准则》以“安全概念和关系”为标题，通过图 2-1 描述了影响信息系统的各要素之间的关系。我国国家标准 GB/T 20984-2007《信息安全技术 信息安全风险评估规范》在该图的基础上，对各要素进行了更为充分的说明，如图 2-2 所示。

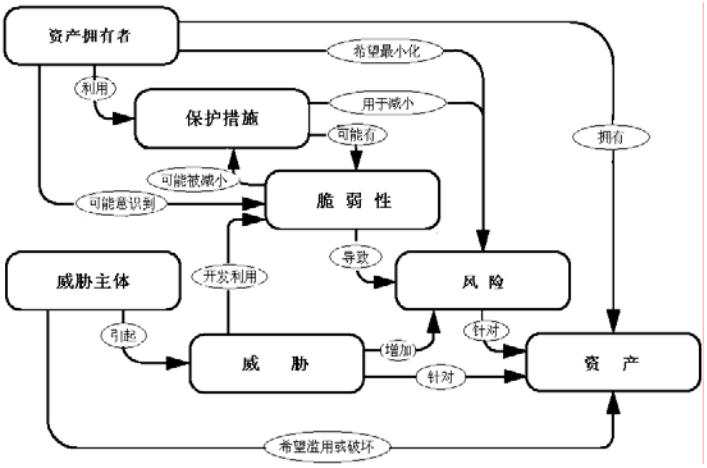


图 2-1 ISO/IEC 15408 给出的信息系统安全各要素之间的关系图

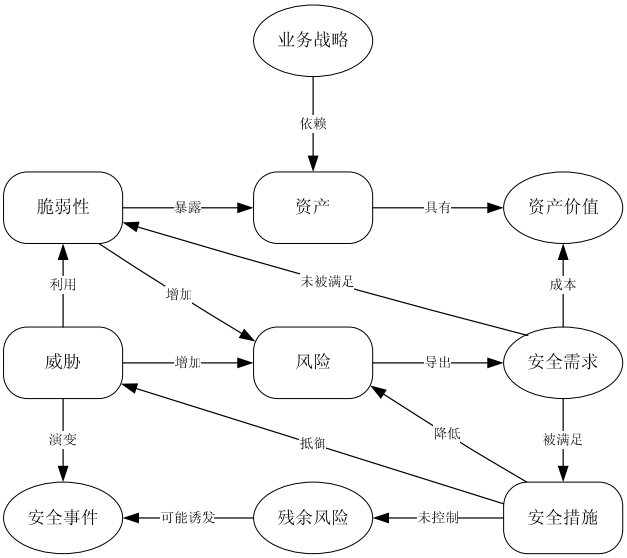


图 2-2　我国国家标准给出的信息系统各要素间的关系图

下面以图 2-2 为基础阐释各要素之间的关系：

1）一个组织的使命通过其业务战略去实现，而业务战略对资产具有依赖性，依赖程度越高，要求其风险越小；

2）资产是有价值的，组织的业务战略越重要，其对资产的依赖程度越高，资产价值就越大；

3）风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成为安全事件；

4）资产的脆弱性可能暴露资产的价值，资产具有的脆弱性越多则风险越大；

5）脆弱性揭示了未被满足的安全需求，威胁会利用脆弱性危害资产；

6）风险的存在及对风险的认识导出了安全需求；

7）安全需求可通过安全措施得以满足，需要结合资产价值考虑其实施成本；

8）安全措施可抵御威胁，降低风险；

9）残余风险是采取了安全措施后仍然存在的风险。这些风险，有的是来源于安全措施不当或无效，需要继续控制的风险；而有些则是在综合考虑了安全成本与效益后不去控制的风险；

10）残余风险应受到密切监视，它可能会在将来诱发新的安全事件。

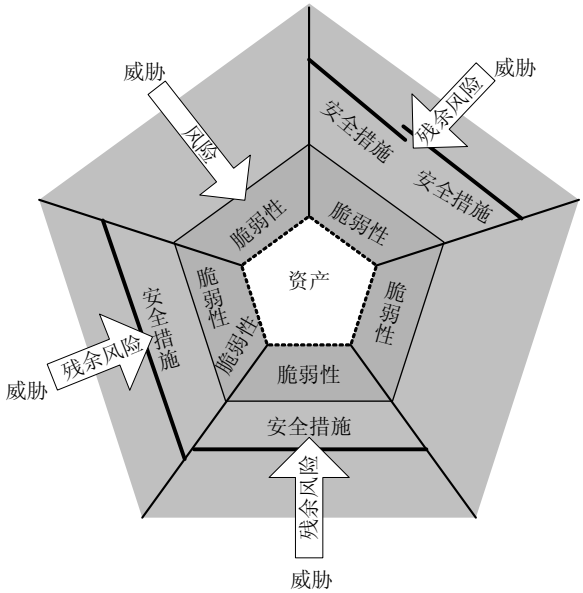


图 2-3　威胁、脆弱性和风险之间的相互作用

图 2-3 从物理角度集中对威胁、脆弱性和风险三者之间的相互作用作了进一步描述：

1）通过安全措施来对资产加以保护，对脆弱性加以弥补，从而可降低风险；

2）实施了安全措施后，威胁只能造成残余风险；

3）往往需要多个安全措施共同起作用；

4）某些情况下，也可能会有多个脆弱性被同时利用；

5）脆弱性与威胁是独立的，威胁要利用脆弱性才能造成安全事件。但有时，某些脆弱性可以没有对应的威胁，这可能是由于这个威胁不在单位考虑的范围内，或者这个威胁的影响极小，以至忽略不计；

6）采取安全措施的目的是控制风险，将残余风险限制在能够接受的程度上。

2.1.3　信息安全风险控制

对信息系统进行安全保护的过程实质上便是对风险进行控制的过程。常见的风险控制措施有四种：

- 风险降低：实施安全措施，以把风险降低到一个可接受的级别。
- 风险承受：接受潜在的风险并继续运行信息系统。
- 风险规避：通过消除风险的原因和/或后果（如在发现风险后放弃系统某项功能或关闭系统）来规避风险，即不介入风险。
- 风险转移：通过使用其它措施来补偿损失，从而转移风险，如购买保险。

第一种措施是最常见的，但显然这并不是唯一的风险控制措施。即使是采取风险降低措施，可能的方法也有很多种，这决定于造成风险的具体原因，例如风险控制的实施点可以有以下几种：

- 当存在系统脆弱性（缺陷或弱点）时：减少或修补系统脆弱性，降低脆弱性被攻击的可能性；
- 当系统脆弱性可被恶意攻击时：运用层次化保护、结构化设计、管理控制将风险最小化或防止脆弱性被利用；
- 当攻击者的成本小于攻击的可能所得时：运用保护措施，通过提高攻击者成本来降低攻击者的攻击动机（例如使用系统访问控制，限制系统用户的访问对象和行为）。
- 当损失巨大时：运用系统设计中的基本原则及结构化设计、技术或非技术类保护措施来限制攻击的范围，从而降低可能的损失。

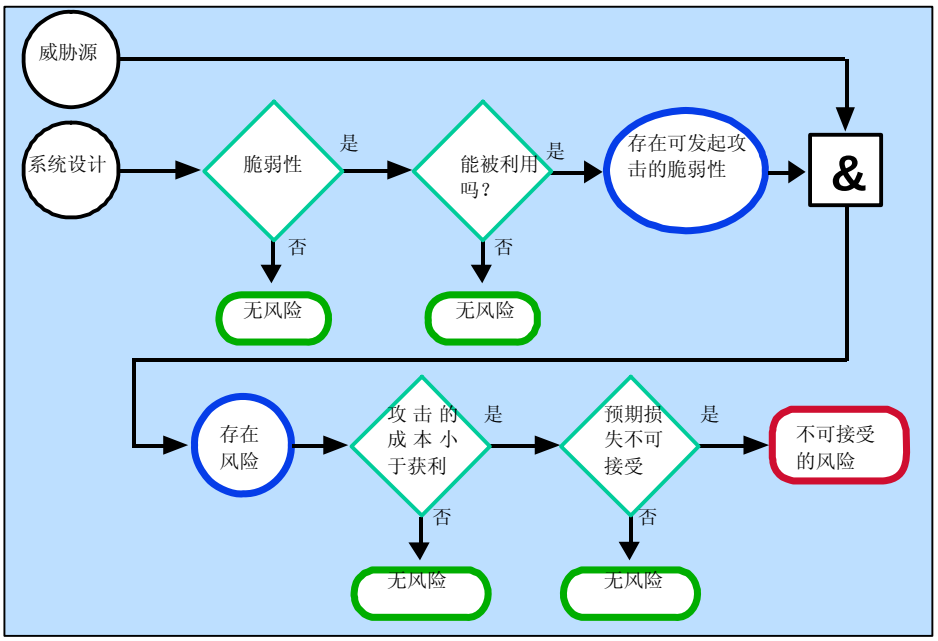


图 2-4　风险控制的实施点

图 2-4 不但阐述了风险控制的实施点，也进一步对威胁、脆弱性和风险的关系作了说明。“&”表示，只有威胁和脆弱性的共同作用才会产生风险。而如果脆弱性不能被利用，或者攻击者的攻击成本大于获利，则都不会造成风险。如果安全事件的损失可以承受（例如这一损失小于安全措施的成本），则也可无视其中的风险。只有在出现了不可接受的风险后，才需要根据产生风险的原因采取针对性措施。

2.2　网络安全基础

网络安全是信息安全中很重要的一部分内容，本章后续章节会介绍网络安全技术，本小节侧重于提供与网络安全有关的必备基础知识。

2.2.1　ISO/OSI 参考模型

ISO/OSI 参考模型是 ISO（国际标准化组织）制定的 OSI（开放系统互连）参考模型，实现了两个异构系统之间的通信，而不管它们底层体系结构如何。OSI 参考模型按功能划分为 7 个层次，从低到高依次为：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，如图 2-5 所示。其中的每一层都定义了相应的功能。

图 2-5　ISO/OSI 参考模型

1．物理层

物理层提供在物理介质上透明的传输比特流所需的各种功能。该层定义了接口和传输介质的机械和电气规范，以及物理设备和接口在传输时所必须执行的过程和功能。

2．数据链路层

数据链路层提供在两个相邻节点间无差错的传输数据帧。该层将一条有可能出差错的信道转变为几乎无差错的数据链路，实现可靠传输。帧是数据链路层的协议数据单元。

3．网络层

网络层确定分组从源端到目的端的路由，负责将源端发出的分组按照路由规则传送到目的端，实现主机到主机的传输。网络层还负责解决网际互连的问题，实现分组跨越多个通信子网的传输。分组是网络层的协议数据单元。

4．传输层

传输层提供端到端的通信，实现透明的报文段传输。报文段是传输层的协议数据单元。

5．会话层

会话层提供在两个通信的应用进程之间建立、维持和同步其交互。它对数据传输进行管理，但不参与具体的数据传输。

6．表示层

表示层主要解决所传输的数据的语法表示。用于数据格式的转化、加密、解密以及压缩等。

7．应用层

应用层直接为用户的应用进程提供服务，对应用进程经常使用的一些功能以及实现这些功能所要使用的协议标准化。互联网的主要应用有：WWW、电子邮件、远程登录、文件传

输等。

ISO/OSI 参考模型从概念和功能上给出了一种异型网络互连的标准框架，概念清楚，指明了每一层上应该做什么事情，也为每一层制定了相应标准，理论较完整。OSI 模型为描述网络提供了详细标准，对统一网络体系结构和协议起到了积极作用，是开发网络协议标准和体系结构的理论框架。但由于其结构复杂，几乎没有厂家生产符合 OSI 标准的网络产品。

图 2-6 给出了基于 OSI 参考模型的数据传输基本过程。

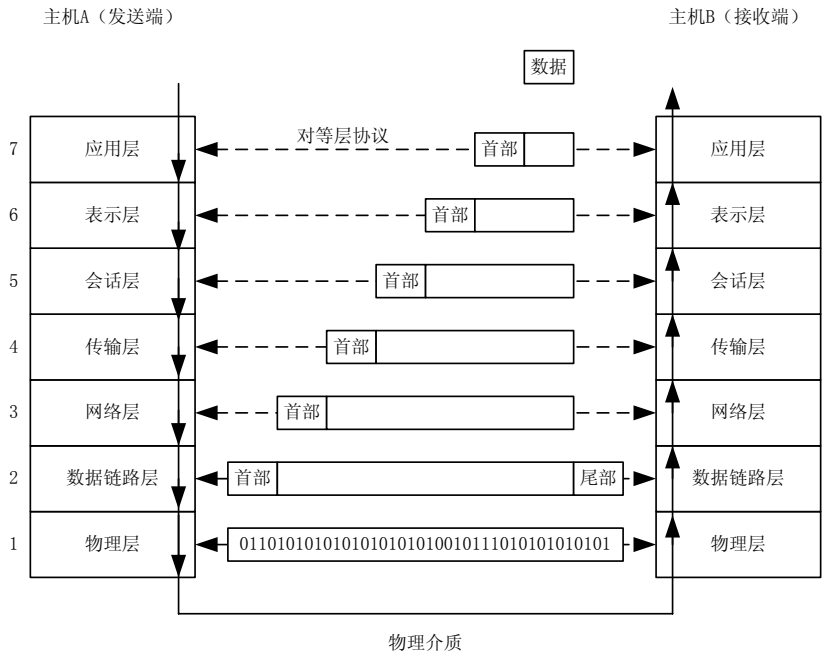


图 2-6　OSI 参考模型中的数据传输基本过程

在图 2-6 中，每一层调用与它直接相邻的下一层提供的服务，同时又向上一层提供服务。例如，第 N 层（例如网络层）调用第 N-1 层（例如数据链路层）提供的服务，同时又向第 N+1 层（例如传输层）提供服务。每一层提供的服务通过该层实体的功能体现出来，上下层只知道服务的调用接口，而不知道具体的实现细节。同一层上的两个实体称作对等实体，通信只在对等实体间进行。每一层对等实体间定义了相应的通信协议，称作对等层协议，协议一般包括首部和数据两个部分，某些协议还可能包含一个尾部。

数据传输过程中，在发送端第 N 层收到 N+1 层传递下来的数据时，都要加上本层协议的首部再传送到第 N-1 层。第 N 层并不知道也不应该知道 N+1 层给它的数据中哪一部分是数据，哪一部分是协议首部，而是把从 N+1 层接收到的协议数据单元看成给本层（N 层）的数据再加上本层的协议首部，组成本层的协议数据单元，传送给它的下一层（N-1 层），这一过程称作封装。封装过程在每一层被重复进行，直至数据到达物理层，然后通过物理介质传输到接收端。

在接收端接收数据时执行一个与封装相反的过程。当从物理层接收到比特串后传递给上一层（例如数据链路层），数据链路层根据预先约定的本层协议规范，区分帧首部和数据部分，把数据部分再传递给上一层（例如网络层），依次过程，每一层收到从相邻的下一层送来的数据后，都要去掉本层协议的首部再向上一层递交，即逐层剥去各首部，直到应用层把数据递交给接收进程。

在图 2-6 中的数据传输过程中，实线箭头方向给出了数据的实际传输方向，在物理介质上进行的是实通信，即比特串实际就在该物理通道上传输，在各对等层实体之间进行的是虚

通信。对于端用户来说，可以把数据传输看作是在对等实体间的直接通信，这样可以简化每一层的设计，体现网络分层体系结构的优点。

2.2.2 TCP/IP 参考模型

TCP/IP 参考模型是一系列协议的集合，也常称作 TCP/IP 协议族。TCP（传输控制协议）和 IP（网际协议）是其中两个最重要的协议，此外该协议族还包括多种其它协议，如应用协议、管理性协议及一些工具性协议。由于 TCP/IP 协议族的开发先于 OSI 参考模型，所以其层次结构不能准确地对应到 OSI 参考模型。随着近年来互联网的迅速发展和普及，作为其支撑协议的 TCP/IP 协议族得到了广泛的应用和推广，它已成为事实上的国际标准和公认的工业标准。

TCP/IP 协议族由 5 层构成，从低到高依次为：物理层、数据链路层、网络层、传输层和应用层。其中，前 4 层和 OSI 参考模型的前 4 层相对应，应用层对应 OSI 参考模型中的上 3 层。图 2-7 给出了 TCP/IP 协议族的主要层次结构，每一层的功能由一个或多个协议实现。

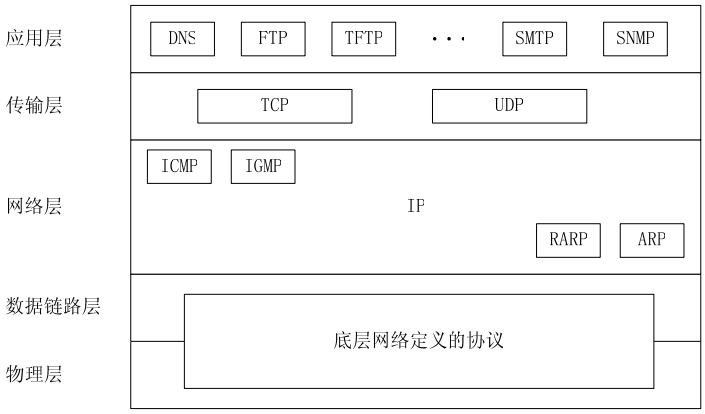


图 2-7　TCP/IP 协议族的层次结构

TCP/IP 协议族的每一层都包含了一些相对独立的协议，实际使用中可以对不同层的协议进行配套使用。每一层的协议都是被它的一个或多个下层协议所支持，同时又为上层协议提供服务。

1．物理层和数据链路层

物理层和数据链路层的协议由底层网络定义，TCP/IP 协议族没有定义任何特定的协议。TCP/IP 互连的底层网络可以包括局域网、城域网和广域网。

2．网络层

IP 协议是网络层的主要协议，提供一种不可靠的、尽最大努力交付的服务。IP 协议是主机到主机的协议，根据网络层路由表实现分组路由，把分组从一个物理设备交付到另一个物理设备。在 IP 协议之上可以有多个传输协议，每个协议为应用程序提供不同类型的服务。

网络层还包含了一些其它协议，如 ARP（地址转换协议）和 RARP（逆地址转换协议）实现 IP 地址与物理地址的相互转换，ICMP（互联网控制报文协议）实现网络层的差错报告和查询报告，IGMP（互联网组管理协议）是多播路由中必不可少的协议，用于多播路由器和实现多播的站点之间进行群组成员关系的通信。在网络层中还有一类路由协议，如 RIP（路由信息协议）和 OSPF（开放最短路径优先协议）等用于动态生成路由表。

3．传输层

传输层包括两种协议：TCP（传输控制协议）和 UDP（用户数据报协议）。TCP 提供面向连接的、可靠的传输服务。UDP 提供无连接服务，不能保证数据报传输的可靠性。TCP 和 UDP 协议都使用相同的网络层 IP 协议。

TCP 和 UDP 协议实现进程到进程间的通信，也被称为端到端的协议。两种协议分别适

用不同的应用场合，如 TCP 协议应用于可靠传输的情况，而 UDP 协议应用于实时性要求较高的情况。

4．应用层

应用层包含了各种直接针对用户需求的协议，每个应用层协议都是为了解决某一类应用问题而设计的。例如，DNS（域名服务系统）用于实现域名和 IP 地址的对应；FTP（文件传输协议）用于实现传输文件的功能；SMTP（简单邮件传送协议）用于实现电子邮件的发送；SNMP（简单网络管理协议）用于实现网络管理的需要。

2.2.3 开放系统互联安全体系结构

开放系统互连安全体系结构的研究始于 1982 年，于 1988 年完成，其标志性成果是 ISO 在 1988 年发布了 ISO7498-2 标准。这是基于 OSI 参考模型的 7 层协议之上的一种网络安全体系结构。该标准的核心内容是，为了保证异构计算机进程之间远距离交换信息的安全，定义了系统应当提供的 5 类安全服务和 8 种安全机制，确定了安全服务与安全机制之间的关系以及在 OSI 参考模型中安全服务和安全机制的配置，另外还确定了 OSI 的安全管理。图 2-8 给出了 ISO7498-2 中协议层次、安全服务与安全机制之间的三维空间关系。

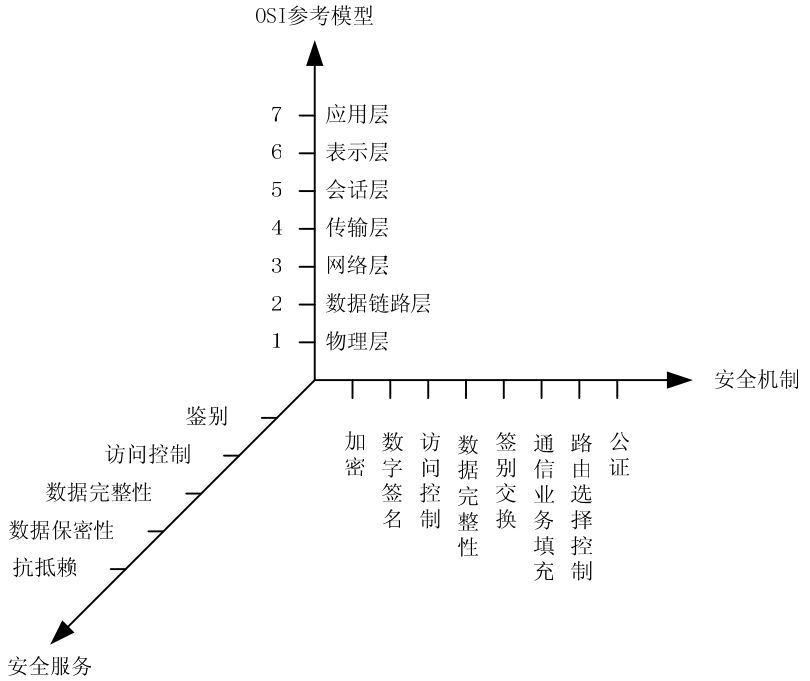


图 2-8　ISO7498-2 协议层次、安全服务与安全机制关系

在 1995 年，ISO7498-2 被等同采用为我国的国家推荐标准 GB/T 9387.2-1995《信息处理系统 开放系统互连 基本参考模型——第二部分：安全体系结构》。

1．安全服务

1）鉴别

鉴别服务提供对通信中的对等实体和数据来源的鉴别，分为对等实体鉴别和数据原发鉴别两种。

对等实体鉴别是确认通信中的对等实体是所需要的实体。这种服务当由（N）层提供时，将使（N+1）实体确信与之打交道的对等实体正是它所需要的（N+1）实体。这种服务在连接建立或在数据传送阶段的某些时刻提供使用，用以证实一个或多个连接实体的身份。使用这种服务可以（仅仅在使用时间内）确信：一个实体此时没有试图冒充别的实体，或没有试图将先前的连接作非授权地重演。

数据原发鉴别是确认通信中的数据来源是所需要的实体。这种服务当由（N）层提供时，

将使（N+1）实体确信数据来源正是所要求的对等（N+1）实体。数据原发鉴别服务对数据单元的来源提供确认。这种服务对数据单元的重复或篡改不提供鉴别保护。

2）访问控制

访问控制服务可以对付 OSI 可访问资源受到的非授权使用，这种保护服务可应用于对资源的各种不同类型的访问（例如：使用通信资源；读、写或删除信息资源；处理资源的执行）或应用于对一种资源的所有访问。

3）数据保密性

数据保密性服务对数据提供保护使之不被非授权地泄露。具体分为以下 4 种：

（1）连接保密性。这种服务为一次（N）连接上的全部（N）用户数据保证其保密性。

（2）无连接保密性。这种服务为单个无连接的 N 层服务数据单元（SDU）中的全部（N）用户数据保证其保密性。

（3）选择字段保密性。这种服务为那些被选择的字段保证其保密性，这些字段或处于（N）连接的（N）用户数据中，或为单个无连接的（N）SDU 中的字段。

（4）通信业务流保密性。这种服务提供的保护，使得通过观察通信业务流而不可能推断出其中的保密信息。

4）数据完整性

数据完整性服务用来对付主动威胁。具体分为以下 5 种：

（1）带恢复的连接完整性。这种服务为（N）连接上的所有（N）用户数据保证其完整性，并检测整个 SDU 序列中的数据遭到的任何篡改、插入、删除，或同时进行补救和/或恢复。

（2）不带恢复的连接完整性。与上带恢复的连接完整性中的服务相同，只是不作补救恢复。

（3）选择字段的连接完整性。这种服务为在一次连接上传送的（N）SDU 的（N）用户数据中的选择字段保证其完整性，所取形式是确定这些被选字段是否遭到了篡改、插入、删除或不可用。

（4）无连接完整性。这种服务当由（N）层提供时，对发出请求的那个（N+1）实体提供完整性保证。无连接完整性服务为单个的无连接 SDU 保证其完整性，所取形式可以是确定一个接受到的 SDU 是否遭受了篡改。另外，在一定程度上也能提供对连接重放的检测。

（5）选择字段无连接完整性。这种服务为单个无连接的 SDU 中的被选字段保证其完整性，所取形式为确定被选字段是否遭受了篡改。在一次连接上，连接开始时使用对等实体鉴别服务，并在连接的存活期使用数据完整性服务就能联合起来为在此连接上传送的所有数据单元的来源提供确证，为这些数据单元的完整性提供确证，而且，例如使用顺序号，还能为数据单元的重复提供检测。

5）抗抵赖

抗抵赖服务可取如下两种形式，或两者之一：

（1）有数据原发证明的抗抵赖。即为数据的接收者提供数据来源的证据，这将使发送者谎称未发送过这些数据或否认它的内容的企图不能得逞。

（2）有交付证明的抗抵赖。即为数据的发送者提供数据交付证据。这将使得接收者事后谎称未收到过这些数据或否认它的内容的企图不能得逞。

2．安全机制

1）加密机制

加密既能为数据提供保密性，也能为通信业务流信息提供保密性，并且还成为本小节中所介绍的其它安全机制起补充作用。

2）数字签名机制

数字签名机制确定两个过程：（1）对数据单元签名；（2）验证签过名的数据单元。

第一个过程使用签名者所私有的（即独有的和保密的）信息。第二个过程所用的程序与信息是公之于众的，但不能够从它们推断出该签名者的私有信息。有关加密和签名的知识可详见第 3 章。

3）访问控制机制

为了判断和实施一个实体的访问权，访问控制机制可以使用该实体已鉴别过的身份，或使用有关该实体的信息（例如它与一个已知的实体集的从属关系），或使用该实体的权力。如果这个实体试图使用非授权的资源，或者以不正当方式使用授权资源，那么访问控制功能将拒绝这一企图，另外还可能产生一个报警信号或将其记录下来。

访问控制机制可以建立在以下一种或多种手段之上。

- 访问控制信息库：在这里保存有对等实体的访问权限。这些信息可以由授权中心保存，或由正被访问的实体保存。信息的形式可以是一个访问控制表，或者等级结构的矩阵。还要预先假定对等实体的鉴别已得到保证。
- 鉴别信息：例如口令，对这一信息的占有和出示便证明正在进行访问的实体已被授权。
- 权力：对它的占有和出示便证明有权访问由该权力所规定的实体或资源。权力应是不可伪造的并以可信赖的方式进行运送。
- 安全标记：当与一个实体相关联时，这种安全标记可用来表示同意或拒绝访问，通常根据安全策略而定。
- 试图访问的时间。
- 试图访问的路由。
- 访问持续期。

4）数据完整性机制

数据完整性有两个方面：一是单个数据单元或字段的完整性，二是数据单元流或字段流的完整性。一般来说，用来提供这两种类型完整性服务的机制是不相同的。

决定单个数据单元的完整性涉及两个过程，一个在发送实体上，一个在接收实体上。发送实体给数据单元附加上一个量，这个量为该数据的函数。这个量可以是分组校验码那样的补充信息，或是一个密码校验值，而且它本身可以被加密。接收实体产生一个相应的量，并把它与接收到的那个量进行比较以决定该数据是否在传送中被篡改过。单靠这种机制不能防止单个数据单元的重放。在网络体系结构的适当层上，操作检测可能在本层或较高层上导致恢复作用（例如重传或纠错）。

对于连接方式数据传送，保护数据单元序列的完整性（即防止乱序、数据的丢失、重放、插入和篡改）还另外需要某种明显的排序形式，例如顺序号、时间标记或密码链。

对于无连接数据传送，时间标记可以用来在一定程度上提供保护，防止个别数据单元的重放。

5）鉴别交换机制

可用于鉴别交换的一些技术是：使用鉴别信息，例如口令，由发送实体提供而由接收实体验证；密码技术；使用该实体的特征或占有物。

鉴别交换机制可设置在（N）层以提供对等实体鉴别。如果在鉴别实体时，这一机制得到否定的结果，就会导致连接的拒绝或终止，也可能在安全审计跟踪中增加一个记录，或给安全管理中心一个报告。

当采用密码技术时，这些技术可以与“握手”协议结合起来以防止重放（即确保存活期）。

鉴别交换技术的选用取决于使用它们的环境。在许多场合，它们必须与下列各项结合使用：时间标记与同步时钟；两方握手和三方握手（分别对应于单方鉴别和相互鉴别）；由数

字签名和公证机制实现的抗抵赖服务。

6）通信业务填充机制

通信业务填充机制能用来提供各种不同级别的保护，抵抗通信业务分析。这种机制只有在通信业务填充受到保密性服务保护时才是有效的。

7）路由选择控制机制

路由能动态地或预定地选取，以便只使用物理上安全的子网络、中继站或链路。

在检测到持续的操作攻击时，端系统可希望指示网络服务的提供者经不同的路由建立连接。

带有某些安全标记的数据可能被安全策略禁止通过某些子网络、中继站或链路。连接的发起者（或无连接数据单元的发送者）可以指定路由选择说明，由它请求回避某些特定的子网络、链路或中继站。

8）公证机制

有关在两个或多个实体之间通信的数据的性质，如它的完整性、原发、时间和目的地等能够借助公证机制而得到确保。这种保证是由第三方公证人提供的。公证人为通信实体所信任，并掌握必要信息以一种可证实方式提供所需的保证。每个通信事例可使用数字签名、加密和完整性机制以适应公证人提供的那种服务。当这种公证机制被用到时，数据便在参与通信的实体之间经由受保护的通信事例和公证方进行通信。

3．安全服务与安全机制的关系

ISO 7498-2 标准说明了实现哪类安全服务应该采用哪种（些）安全机制。一般来说，一类安全服务可以通过某种安全机制单独提供，也可以通过多种安全机制联合提供；一种安全机制也可以提供一类或多类安全服务。表 2-1 说明了安全服务与安全机制之间的关系。

表 2-1　OSI 安全服务与安全机制的关系

安全服务		安全机制							
		加密	数字签名	访问控制	数据完整性	签别交换	通信业务填充	路由选择控制	公证
鉴别	对等实体鉴别	Y	Y	-	-	Y	-	-	-
	数据原发鉴别	Y	Y	-	-	-	-	-	-
访问控制	访问控制	-	-	Y	-	-	-	-	-
保密性	连接保密性	Y	-	-	-	-	-	Y	-
	无连接保密性	Y	-	-	-	-	-	Y	-
	选择字段保密性	Y	-	-	-	-	-	-	
	通信业务流保密性	Y	-	-	-	-	Y	Y	-
完整性	带恢复的连接完整性	Y	-	-	Y	-	-	-	-
	不带恢复的连接完整性	Y	-	-	Y	-	-	-	-
	选择字段连接完整性	Y	-	-	Y	-	-	-	
	无连接完整性	Y	Y	-	Y	-	-	-	-
	选择字段无连接完整性	Y	Y	-	Y	-	-	-	-
抗抵赖	有数据原发证明的抗抵赖	-	Y	-	Y	-	-	-	Y
	有交付证明的抗抵赖	-	Y	-	Y	-	-	-	Y

说明：Y 表示安全服务可由该机制提供；-表示不提供。

4．安全管理

OSI 安全管理涉及两个方面：与 OSI 有关的安全管理；OSI 管理的安全。OSI 安全管理与这样一些操作有关，它们不是正常的通信情况但却为支持与控制这些通信的安全所必需。

由分布式开放系统的行政管理强加的安全策略可以是各种各样的，OSI 安全管理标准应该支持这样的策略。从属于单一的安全策略、受单个授权机构管理的多个实体构成的集合称

之为“安全域”。安全域是信息安全中的重要概念。

OSI 安全管理涉及到 OSI 安全服务的管理与安全机制的管理。这样的管理要求给这些服务与机制分配管理信息，并收集与这些服务和机制的操作有关的信息。例如，密钥的分配，设置行政管理强加的安全选择参数，报告正常的与异常的安全事件（审计跟踪），以及服务的激活与停止。安全管理并不强调在呼叫特定的安全服务的协议中（例如连接请求的参数中）传递与安全有关的信息。

SMIB（安全管理信息库）是一个概念上的集存地，存储开放系统所需的与安全有关的全部信息。这一概念对信息的存储形式与实施方式不提出要求。但是每个端系统必须包含必需的本地信息，使其能执行某个适当的安全策略。SMIB 在端系统的一个（逻辑的或物理的）组中执行一种协调的安全策略是必不可少的，在这一点上，SMIB 是一个分布式信息库。在实际中，SMIB 的某些部分可以与 MIB（管理信息库）结合成一体，也可以分开。SMIB 有多种实现办法，例如，数据表、文卷、嵌入实开放系统软件或硬件中的数据或规则。

安全管理可以要求在不同系统的行政管理机构之间交换与安全有关的信息，以便使 SMIB 得以建立或扩充。在某些情况下，与安全有关的信息将经由非 OSI 通信通路传递，局部系统的管理者也将采用非 OSI 标准化方法来修改 SMIB。在另外一些情况下，可能希望在一个 OSI 通信通路上交换这样的信息，这时这些信息将在运行于实开放系统中的两个安全管理应用之间传递。该安全管理应用将使用这些通信信息来修改 SMIB。SMIB 的这种修改可以要求事先给适当的安全管理者授权。

应用协议将为在 OSI 通信信道上交换与安全有关的信息作出规定。

OSI 安全管理活动可分为三类：系统安全管理；安全服务管理；安全机制管理。另外，还必须考虑到 OSI 管理本身的安全。对这几类安全管理所执行的关键功能概述如下。

1）系统安全管理

系统安全管理涉及总的 OSI 环境安全方面的管理。属于这一类安全管理的典型活动如下：

- 总体安全策略的管理，包括一致性的修改与维护。
- 与别的 OSI 管理功能的相互作用。
- 与安全服务管理和安全机制管理的交互作用。
- 事件处理管理，包括远程报告那些违反系统安全的明显企图，以及对用来触发事件报告的阈值的修改。
- 安全审计管理，包括选择将被记录和被远程收集的事件，授予或取消对所选事件进行审计跟踪日志记录的能力，所选审计记录的远程收集，准备安全审计报告。
- 安全恢复管理，包括维护那些用来对实有的或可疑的安全事故作出反应的规则，远程报告对系统安全的明显违反，安全管理者的交互作用。

2）安全服务管理

安全服务管理涉及特定安全服务的管理。在管理一种特定安全服务时可能执行的典型活动如下：

- 为该种服务决定与指派安全保护的目标。
- 指定与维护选择规则（存在可选情况时），用以选取为提供所需的安全服务而使用的特定的安全机制。
- 对那些需要事先取得管理同意的可用安全机制进行协商。
- 通过适当的安全机制管理功能调用特定的安全机制，例如，用来提供行政管理强加的安全服务。
- 与别的安全服务管理功能和安全机制管理功能的交互作用。

3）安全机制管理

安全机制管理涉及的是特定安全机制的管理。典型的安全机制管理功能如下：

（1）密钥管理。包括：间歇性地产生与所要求的安全级别相称的合适密钥；根据访问控制的要求，对于每个密钥决定哪个实体应该接受密钥的拷贝；用可靠办法使这些密钥对实开放系统中的实体实例是可用的，或将这些密钥分配给它们。某些密钥管理功能将在 OSI 环境之外执行。这包括用可靠手段对密钥进行物理的分配。

（2）加密管理。包括：与密钥管理的交互作用；建立密码参数；密码同步。密码机制的存在意味着使用密码管理，和采用共同的方式调用密码算法。

（3）数字签名管理。包括：与密钥管理的交互作用；建立密码参数与密码算法；在通信实体与可能的第三方之间使用协议。一般说来，数字签名管理与加密管理极为类似。

（4）访问控制管理。包括：可涉及到安全属性（包括口令）的分配，或对访问控制表或权力表进行修改。也可能涉及到在通信实体与其它提供访问控制服务的实体之间使用协议。

（5）数据完整性管理。包括：与密钥管理的交互作用；建立密码参数与密码算法；在通信的实体间使用协议。当对数据完整性使用密码技术时，数据完整性管理便与加密管理极为类似。

（6）鉴别管理。包括：把说明信息，口令或密钥（使用密钥管理）分配给要求执行鉴别的实体。它也可以包括在通信的实体与其它提供鉴别服务的实体之间使用协议。

（7）通信业务填充管理。包括：预定的数据率；指定随机数据率；指定报文特性，例如长度；可能按日时间或日历来改变这些规定。

（8）路由选择控制管理。包括确定那些按特定准则被认为是安全可靠或可信任的链路或子网络。

（9）公证管理。包括：分配有关公证的信息；在公证方与通信的实体之间使用协议；与公证方的交互作用。

4）OSI 管理的安全

所有 OSI 管理功能的安全以及 OSI 管理信息的通信安全是 OSI 安全的重要部分。这一类安全管理将借助对上面所列的 OSI 安全服务与机制作适当的选取以确保 OSI 管理协议与信息获得足够的保护。例如，在管理信息库的管理实体之间的通信一般将要求某种形式的保护。

5）特定的系统安全管理活动

特定的系统安全管理活动有以下几类：

（1）事件处理管理。包括远程报告那些违反系统安全的明显企图，以及对用来触发事件报告的阈值的修改。

（2）安全审计管理。包括：选择将被记录和被远程收集的事件；授予或取消对所选事件进行审计跟踪日志记录的能力；所选审计记录的远程收集；准备安全审计报告。

（3）安全恢复管理。包括：维护那些用来对实有的或可疑的安全事故作出反应的规则；远程报告对系统安全的明显违反；安全管理者的交互作用。

5．OSI 安全体系到 TCP/IP 的映射

ISO 7498-2 是基于开放系统互连参考模型之上构建的安全体系结构，TCP/IP 模型中的每一层对应于 OSI 参考模型中的一层或多层。可以将 ISO 7498-2 安全体系结构中的安全服务和安全机制映射到 TCP/IP 模型中，如表 2-2 给出了安全服务与 TCP/IP 协议层次之间的关系。

表 2-2　安全服务与 TCP/IP 参考模型协议层之间的关系

安全服务		TCP/IP 协议层			
		物理链路层	网络层	传输层	应用层
鉴别	对等实体鉴别	-	Y	Y	Y

	数据原发鉴别	-	Y	Y	Y
访问控制	访问控制	-	Y	Y	Y
保密性	连接保密性	Y	Y	Y	Y
	无连接保密性	Y	Y	Y	Y
	选择字段保密性	-	-	-	Y
	通信业务流保密性	Y	Y	-	Y
完整性	带恢复的连接完整性	-	-	Y	Y
	不带恢复的连接完整性	-	Y	Y	Y
	选择字段连接完整性	-	-	-	Y
	无连接完整性	-	Y	Y	Y
	选择字段无连接完整性	-	-	-	Y
抗抵赖	有数据原发证明的抗抵赖	-	-	-	Y
	有交付证明的抗抵赖	-	-	-	Y

说明：Y 表示该安全服务应该在相应的层中提供；-表示不提供。

2.3 信息安全保障体系

所谓信息安全保障体系，是指实施信息安全保障的法制、组织管理和技术等层面有机结合的整体，是信息社会国家安全的基本组成部分，是保证国家信息化顺利进行的基础。

构建信息安全保障体系是一种持续建设、与时俱进的过程，不能一劳永逸。衡量信息安全保障体系成功与否的标准，不仅要看是否取得了物质结果，更要注重是否形成了高效的机制与持续发展的能力。例如，国家信息安全保障体系不但要求拥有足够的信息安全专业人才，更要加强学科建设；不但要求制定必需的信息安全法律法规，更要建立及时掌握信息安全立法需求、协调法律关系的良性机制。

2.3.1 概述

信息安全保障体系是国家信息安全保障工作的着眼点，是国家信息安全保障能力的载体。如图 2-9 所示，国家信息安全保障体系的目标是实现“一个重点确保”，其内容是建设“四个层面”，满足“两个支撑”条件：

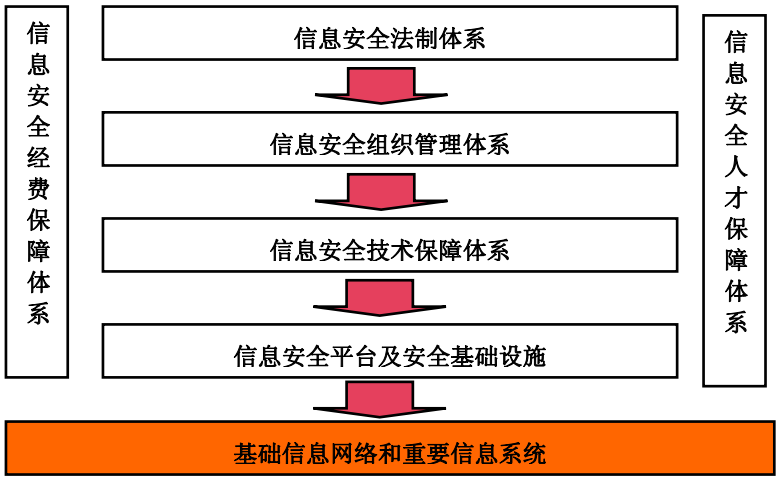


图 2-9 信息安全保障体系

- 一个确保：
  - ✓ 重点确保国家基础信息网络和重要信息系统的安全，创建安全健康的网络环境
- 四个层面：

- ✓ 信息安全法制体系
- ✓ 信息安全组织管理体系
- ✓ 信息安全技术保障体系
- ✓ 信息安全平台及安全基础设施

- 两个支撑：
  - ✓ 信息安全经费保障体系
  - ✓ 信息安全人才保障体系

2.3.2 一个确保

信息安全保障体系的重点目标，就是确保基础信息网络和重要信息系统的安全，创建安全健康的网络环境。

基础信息网络包括广播电视网、电信网以及公共互联网等通信基础设施，重要信息系统是对国计民生、社会稳定、公共利益、国家安全有重大影响的信息系统，包括银行、保险、证券、电力、铁路、民航、供水、供气、石油和天然气管道运输等单位以及国家机关、国家重点科研机构和重大工程的信息系统。基础信息网络和重要信息系统的安全，就是要求网络与信息系统能够正常运行，不因人为或偶然的因素而被中断、破坏、修改或被恶意利用，网络与信息系统中存储、处理和传输的数据不被非法窃取、泄露、篡改或删除。

创建安全健康的网络环境，是指利用网络和信息系统制作、发布、复制或传播的信息符合有关法律、法规的规定，不对国家安全、公共秩序和社会稳定造成危害，不含有淫秽、色情、虚假或欺诈内容，不侵犯个人或组织的合法权益，不违背中华民族优良文化传统习惯和社会公德，从而充分发挥互联网等信息网络在中国社会主义文化建设中的重要作用，创建民主法治、公平正义、诚信友爱、充满活力又安定有序的互联网和谐发展环境。

2.3.3 四个层面

信息安全保障体系的四个层面包括信息安全法制体系、信息安全组织管理体系、信息安全技术保障体系和信息安全平台及安全基础设施。

1．信息安全法制体系

信息安全法制体系的基本内容是确立信息安全领域的法规框架，加强执法能力，做到有法可依，有法必依。

确立信息安全法规框架，就是确立我国信息安全领域的基本法律原则、基本法律责任和基本法律制度，系统、全面地解决我国信息安全立法中的基本问题，从不同层次妥善处理信息安全各方主体的权利义务关系，规范公民、法人和其他组织的信息安全行为，明确信息安全的执法主体及其职责，为各职能部门的工作提供执法依据。

信息安全立法工作应遵循以下基本原则：一是构成体系的各个法律、法规、规章相互之间应当协调一致，相互补充；二是明确信息安全的执法主体，以及信息安全各方主体的安全责任、义务和安全措施，使其具有可操作性；三是增强立法的适应性，尽可能调整信息安全出现的新问题；四是应当具有前瞻性和灵活性，为信息安全的发展变化留有余地；五是不超过合法范围对信息安全事项进行行政许可。

除立法工作外，信息安全法制建设的要点还包括按照权力与责任相一致、权力与利益相分离的要求，建立权责明确、行为规范、监督有效、保障有力的执法体制。信息安全执法活动必须严格按照法律规定的权限和程序进行，正确行使权力和履行职责，保护企业和公民的合法权益，打击网络违法犯罪。要把监控有害信息内容工作法制化，依法保护公民通信自由和隐私，通过法律程序维护信息内容安全。

2．信息安全组织管理体系

“坚持管理与技术并重”是我国信息安全保障工作的主要原则之一，这是对信息安全管理与技术之间辩证关系的新的认识。

管理学界对“管理”的定义多种多样，不一而足，但毫无疑问的是，任何一种管理活动都必须明确谁来管（即管理主体）、管什么（即管理客体）、怎么管（即管理手段）以及管得怎么样（管理效果）的问题。信息安全管理则是指把分散的信息安全技术因素和人的因素，通过策略、规则协调整合成为一体，服务于信息化的使命。

信息安全管理的层次性。根据管理主体、管理客体等要素的不同，信息安全管理分为两个层次：

一是国家层次的信息安全管理。其管理的主体是代表国家意志的信息安全相关行政主管部门，这些部门依法行使本部门对信息安全的管理职责，以战略方针、政策、法规、标准和其它措施为基本手段，重在创造良好的信息化和信息安全政策环境，有效分配国家和社会资源，积极调整各方关系，加强信息安全技术组织与建设，从宏观和全局角度推动信息安全保障各项工作的落实。这种信息安全管理的重点是强化国家行政层面的信息安全管理机构的职能，建立高效、职责分工明确的行政管理和业务组织体系，加强国家信息安全保障的综合协调工作。此外，还应落实“谁主管谁负责、谁运营谁负责”的原则，建立健全信息安全责任制。

另一种则是一个组织内部的信息安全管理。其管理的主体是组织内的管理层，管理的对象是“人”和“技术”，管理的核心目标是建立本单位信息安全管理体系，合理控制信息安全风险。其基本任务分为两个方面：通过信息安全管理措施直接满足信息安全需求；通过信息安全管理过程驱动信息安全技术的实施。

由于信息化有通过网络互连、互通、互操作的特点，没有强力度的全局安全管理，仅靠局部是难以发挥信息化应有的效率和效益的。因此，宏观信息安全管理是信息化社会有序健康运作的保证，是技术发展的推动力，是把分散的信息保障能力由“指头”变成“拳头”的聚合剂。另一方面，由于现代信息系统是人机结合的复杂系统，没有细粒度的对人和技术的有效安全管理，则系统的效率和效益难以发挥。因此，微观信息安全管理是人如何操作技术的规范尺度，是发挥人的因素和技术因素的桥梁。宏观管理是对微观管理的指导和约束，微观管理是对宏观管理的贯彻和落实，二者紧密相关，互为依托，缺一不可。

3．信息安全技术保障体系

国家信息安全技术保障体系是国家信息安全保障体系的重要组成部分。建设我国信息安全技术保障体系，核心是要加强自主可控的信息安全核心技术的研发，摆脱在操作系统、芯片、高端通信设备等信息技术产品方面受制于人的局面。我国信息技术水平总体上距国外差距仍较大，应该高度重视信息安全自主创新能力，并抓住可信计算技术等技术革新机遇，谋求信息安全技术的跨越式发展。由于信息化是一种全面渗透到国民经济和社会发展各方面的积极的生产力，封闭攻关的研究模式有违信息化的发展规律。尤其是，国外的很多信息技术已经因市场占有率和使用率而成为事实上的标准，信息化对互联、互通、互操作的本质需求使我们必须正视这一现实情况，除继续加大投资与统筹规划外，必须在自主可控核心技术的研发中改变思路，想方设法发展应用，坚持抓应用、促规模的发展道路，以应用带动我国自主可控的核心技术的发展。

我国应大力持续发展信息安全产业，确保信息安全保障体系建设具有足够的物质基础。应着重抓法制，立标准，创造良好的产业发展环境；增加对信息安全产业发展的资金投入，创造良好的融资环境；建立健全信息安全市场服务体系；加速培养信息安全技术人才，发挥人才的积极性和创造性。

4．信息安全平台及基础设施建设

信息安全平台及基础设施建设的重点，是建立安全事件应急响应中心和容灾备份基础设施；发挥密码在保障体系中的基础和核心作用，加强以密码为基础的信息保护和网络信任体系的建设；建设和完善信息安全监控体系。

建设信息安全应急响应中心的基本内容是通过信息通报和共享机制，采用逐级上报、集中研判、快速预警、统一指挥、紧急处置、追查反制等策略和措施，有效防范、及时控制和消除有害信息传播、计算机病毒感染和网络攻击、网络恐怖活动以及其它紧急突发信息安全事件的危害。建设信息安全容灾备份基础设施的基本内容是坚持统筹规划、资源共享、平战结合的原则，建立远程异地备份中心，及时有效备份重要数据，确保重要数据的可靠保存和随时取用，使信息系统在发生灾难时能够迅速恢复运行。

网络信任体系旨在解决信息网络空间中行为主体的身份真实性、授权与责任认定问题，以建立类似现实生活空间的信任体系，维护信息网络空间的有序运行。针对不同的安全域和安全等级，网络信任体系的构成是不一样的。在电子商务应用环境中，交易双方互不隶属，仅仅依靠交易双方无法实现信任凭证，必须要依靠一个交易双方都认可的可信第三方机构来提供信任证明。而在一个确定组织的内部，工作流程相对固定，操作人员都有明确的上下级垂直组织或生产关系，这决定了其安全授权关系完全是一种明确的上下级关系，不必对完全没有任何隶属关系、需要依靠第三方认证的人员进行授权。这种情况下，网络信任体系的建设不必引入第三方认证模式，只要能够实现身份认证、授权管理和责任认定即可。

信息安全监控体系是指国家为了维护国家安全、公共利益和信息网络安全秩序，在信息系统和信息网络（特别是在互联网）上建立的监视和控制网络攻击、病毒入侵、网络失泄密、有害信息传播的技术平台。在监控体系的建设中，应注意两方面的问题。首先，要明确监控的对象。不同的监控对象（网络攻击、病毒入侵、网络失泄密、有害信息传播），需要的监控技术不同，面临的法律和政策约束也不同，适用的环境也不同。第二，要加强资源利用，避免低水平重复建设。此外，还需加强对技术监控手段的管理，依据法律，严格规范技术监控的审批、范围、期限等，防止技术监控手段的滥用，保护公民、法人和其他组织的合法权益。

2.3.4 两个支撑

国家信息安全保障体系需要两个重要支撑：信息安全经费保障体系和信息安全人才保障体系。

1．信息安全经费保障体系

信息安全工作离不开经费保障，但由于很多信息安全经费投入不会马上见到效益，信息安全经费保障不到位的情况经常出现。信息安全经费保障的重点，是明确信息安全保障体系建设经费占信息化经费的比例。在信息化建设中，信息安全要与信息化同步规划、同步建设、同步发展。各级财政拨款中，应重在建立信息安全经费保障机制，使信息安全建设、运维资金能够及时到位，将信息安全风险评估、信息安全培训等活动所需经费纳入日常运维经费之中，并建立机动资金或预备资金，确保系统测评、应急预案演习、突发事件处置等工作的正常开展。

在信息安全经费保障体系中，还应划拨专项资金，用于支持耗资较大的信息安全基础设施建设。

在保障信息安全经费的同时，必须研究建立对信息安全经费投入进行绩效审计的方法与机制，最大限度发挥信息安全经费投入的效益，避免资金浪费。

2．信息安全人才保障体系

当今世界的竞争，从根本上说是人才的竞争。高素质的人才队伍是信息安全保障体系的智力支撑，应把人才问题摆上信息安全工作的战略位置。

建设信息安全人才保障体系得重点，是面对信息安全工作对复合性人才的需求，努力加强学科建设，推行学历教育，培养信息安全工作急需的科研、工程、管理、法律等多方面人才。要集中优势资源，在高校和科研单位成立若干重点信息安全专业或学院，避免教育资源浪费。此外，还应加大信息安全社会化培训和宣传力度，加强信息安全培训机构建设，提高

全民信息安全素质。

2.4 积极防御的信息安全技术保护框架

当前大部分信息安全系统主要是由防火墙、入侵检测、病毒防范等组成。常规的安全手段只能是在网络层设防，在外围对非法用户和越权访问进行封堵，以达到防止外部攻击的目的。由于这些安全手段缺少对访问者源端——客户机的控制，加之操作系统的不安全导致应用系统的各种漏洞层出不穷，其防护效果正越来越不理想。此外，封堵的办法是捕捉黑客攻击和病毒入侵的特征信息，而这些特征是已发生过的滞后信息，不能科学预测未来的攻击和入侵。随着恶意用户的攻击手段变化多端，防护者只能把防火墙越砌越高、入侵检测越做越复杂、恶意代码库越做越大，误报率也随之增多，使得安全的投入不断增加，维护与管理变得更加复杂和难以实施，信息系统的使用效率大大降低，而对新的攻击毫无防御能力。随着时间的发展，以防火墙、入侵检测、病毒防范这“老三样”为主要手段的这类信息安全保护思路已经越来越显示出被动性，迫切标本兼治的新型的信息安全保护框架。

2.4.1 对当前信息安全保护思路的反思

事实上，产生安全事故的技术原因在于，现在的 PC（个人计算机）机软、硬件结构简化，导致资源可任意使用，尤其是执行代码可修改，恶意程序可以被植入。例如，病毒程序利用了 PC 机操作系统对执行代码不检查一致性的弱点，将病毒代码嵌入到执行代码程序，实现病毒传播；黑客利用被攻击系统的漏洞窃取超级用户权限，植入攻击程序，肆意进行破坏。更为严重的是，系统对合法的用户没有进行严格的访问控制，可以进行越权访问，造成不安全事件。

据国际权威机构统计，83%的信息安全事故为内部人员或内外勾结所为，而且呈上升趋势。因此，应该以“防内为主、内外兼防”的模式，从提高使用节点自身的安全着手，构筑积极、综合的安全防护系统。这种积极防御的基本思路是主动防止非授权访问操作，从客户端操作平台实施高等级防范，使不安全因素从终端源头被控制。这在工作流程相对固定的重要信息系统中显得更为重要而可行。

以我国电子政务网为例，由政务内网和政务外网两部分组成。政务内网是涉密网，处理涉及国家秘密事务。政务外网是非涉密网，是政府的业务专网，主要运营政府部门面向社会的专业性服务和不需要在内网运行的业务。政务内网与政务外网物理隔离，政务外网与互联网逻辑隔离。在电子政务的内外网中，要处理的工作流程都是预先设计好的，操作使用的角色是确定的，应用范围和边界都是明确的。这类工作流程相对固定的生产系统与互联网是有隔离措施的，外部网络的用户很难侵入到内部网络来。

2.4.2 “两个中心”支持下的三重信息安全技术保护框架

在工作流程相对固定的重要信息系统中，信息系统主要由操作应用、共享服务和网络通信三个环节组成。如果信息系统中每一个使用者都是在安全管理支持下经过认证和授权的，其操作都是符合规定的，网络上也不会被窃听和插入，那么就不会产生攻击性的事故，就能够保证整个信息系统的安全，这便构成了工作流程相对固定的生产系统内的信息安全保护框架。

（1）操作应用方面

采用可信客户端确保用户合法性和资源的一致性，使用户只能按照规定权限和访问控制规则进行操作，能做到任何权限级别的人只能做与其身份相符的访问操作，只要控制规则是合理的，那么整个信息系统资源访问过程就是安全的。这样便构成了安全可信的应用环境。

（2）共享服务方面

安全的共享服务边界可以采用安全边界设备（如安全网关等），其应具有身份认证和安全审计功能，将共享服务器（如数据库服务器、WEB 服务器、邮件服务器等）与非法访问

者隔离，防止意外的非授权用户的访问（如非法接入的非可信终端）。这样共享服务端不必做繁重的访问控制，从而减轻服务器的压力，以防止拒绝服务攻击。

（3）网络通信方面

网络通信应该得到全程保护，可以采用 IPSec 协议（缩写 IP Security，是对 IP 协议分组进行加密和认证的通信安全协议）实现网络通信全程安全保密，确保传输连接真实性和数据的保密性、一致性，防止非法窃听和插入。

（4）安全管理方面

重要信息系统的安全级别一般比较高，这要求必须统一管理系统内各个可信客户端的安全策略和设备的配置策略，且集中处理身份标识和认证、安全授权、安全审计、安全事件等信息。此外，密钥的管理和密码服务支持也需要以集中的方式实现。

综上所述，可信的应用操作平台、安全的共享服务资源边界保护、全程安全保护的网络通信和安全管理中心，构成了工作流程相对固定的生产系统的信息安全保护框架。如图 2-10 所示。该图涉及到两个不同的安全域，安全域之间通过安全隔离设备进行连接，安全域之间的通信业通过 IPSec 进行加密。

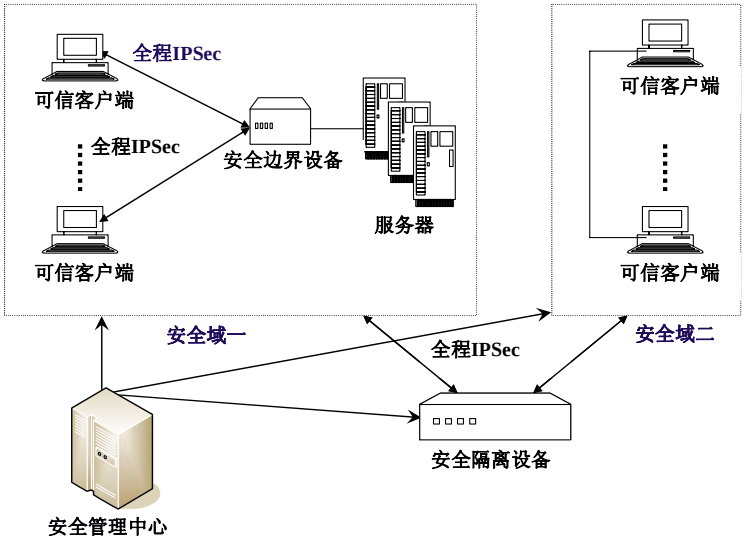


图 2-10　工作流程相对固定的生产系统安全解决方案

综上所述，可在技术层面上将信息系统安全保护分为以下五个环节作为保护重点：

（1）应用环境安全：包括单机、C/S、B/S 模式的安全。采用身份认证、访问控制、密码加密、安全审计等机制，构成可信应用环境。

（2）应用区域边界安全：通过部署边界保护措施控制对内部局域网的访问，实现应用环境之间的安全互联互通。采用安全网关、防火墙等隔离过滤机制，保护共享资源的可信连接。

（3）网络和通信传输安全：确保通信的保密性、一致性和可用性。采用密码加密、完整性校验和实体鉴别等机制，实现可信连接和安全通信。

（4）安全管理中心：提供身份标识和认证、安全授权、实时访问控制策略、审计、事件管理等运行安全服务。

（5）密码管理中心：提供互联互通密码配置、公钥证书和传统的对称密钥的管理，为信息系统提供密码服务支持。

上述五个环节中，之所以不使用“网络边界”的概念，而是考虑“应用区域边界”，是因为安全保护的核心对象是应用，即使在同一网络内部，不同的应用之间也可能有不同的安全需求，需要不同等级的安全防护，特别是各个应用环境的安全策略可能不一致，应用环境

之间必须施加边界保护控制措施。

在跨区域的复杂互联信息系统中，不同应用环境之间可能需要互联，且这些应用环境还与各种类型的公共和专用通信基础设施之间相连，各类应用环境的远程用户也有着不同的远程连接方式。对这种复杂的大型互联系统，可构成三纵（涉密区域、专用区域、公共区域）三横（应用环境、应用区域边界、网络通信）和两个中心（安全管理中心、密码管理中心）为核心内容的信息安全防护框架。如图 2-11 所示。涉密区域、专用区域和公共区域这三种不同安全级别的应用区域在各自采用相应的安全保障措施之后，互相之间有一定的沟通，应该采用安全隔离与信息交换设备进行连接。

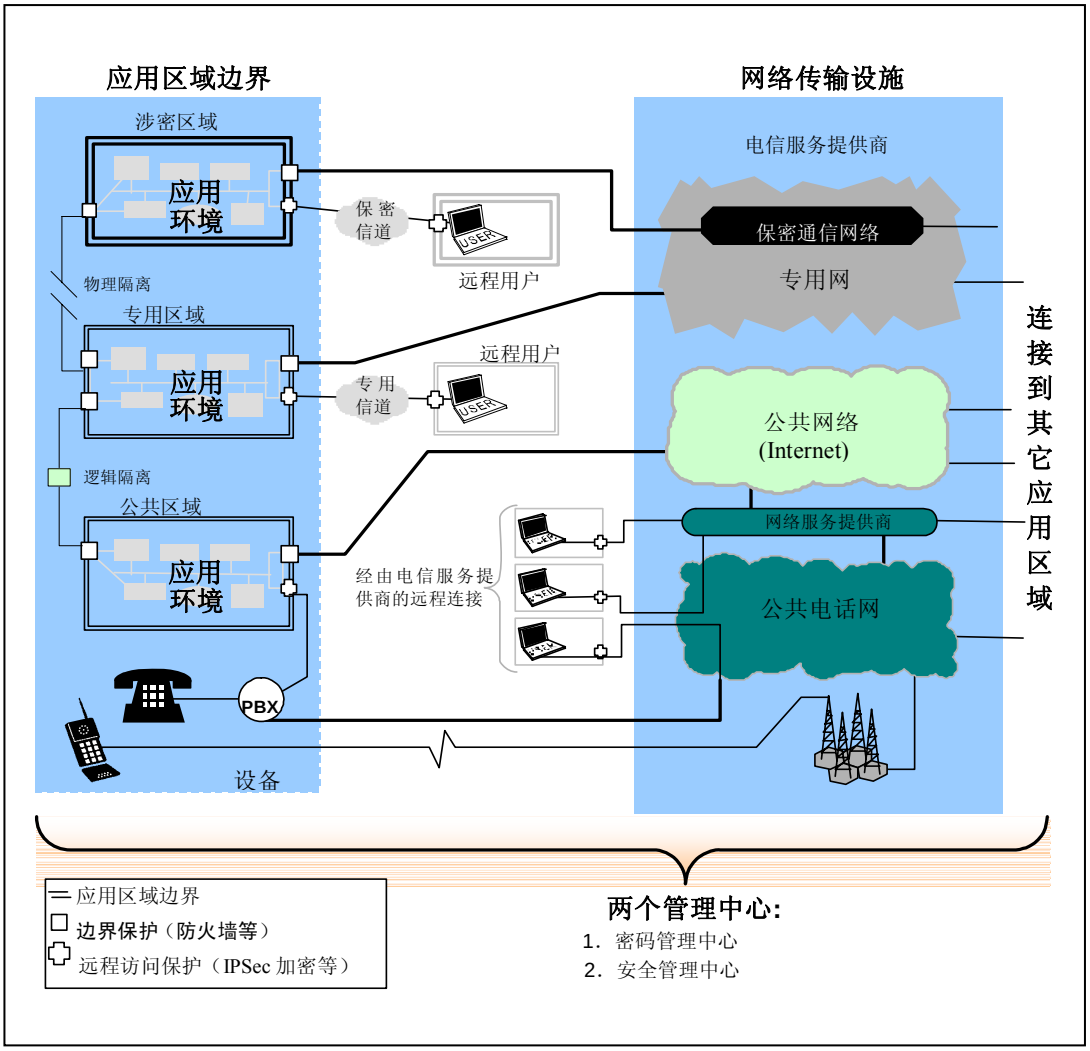


图 2-11　复杂互联系统的信息安全技术保护框架

2.5　常用安全技术

ISO 7498-2 中提出的安全服务可理解为安全需求的一种表示，而信息安全机制是能够提供一种或多种安全服务的、与具体的实现方式无关的且一般不能再细分的安全技术的抽象表示。安全机制一般是“原子”级的，各项机制之间很少出现交叉。信息安全产品则是一种或多种信息安全机制的具体实现。本小结介绍三种常用的信息安全产品，但主要侧重于概念说明。

2.5.1　防火墙

1. 概述

防火墙一词在辞海中的解释是“用非燃烧材料砌筑的墙。设在建筑物的两端或在建筑物内将建筑物分割成区段，以防止火灾蔓延。”在当今的网络环境下，往往借用了这个概念，

使用防火墙来保护敏感的数据不被窃取和篡改，这里的防火墙是由计算机系统来构成的。

防火墙犹如一道护栏隔在被保护的内部网络和不安全的外部网络之间，是一种边界保护的机制，这道屏障的作用就是阻断来自外部的对内部网络的入侵，保护内部网络的安全。

防火墙要起到边界保护作用，需要做到：所有进入内部网络的通信，都必须通过防火墙；所有通过防火墙的通信，都必须经过安全策略的过滤；防火墙自身是安全可靠的，不易被攻破。

2．防火墙的功能

防火墙通常具有如下功能：

1）访问控制功能

访问控制是防火墙最基本也是最重要的功能，通过允许或禁止特定用户对特定资源的访问，保护内部网络资源和数据。

防火墙还可以对所提供的网络服务进行控制，限制一些不安全的服务，减少威胁，提高被保护内部网络的安全性。

2）内容控制功能

防火墙能够对从外部穿越防火墙的数据内容进行控制，阻止不安全的内容进入内部网络，防止内部网络的安全性收到影响。例如，防火墙可以从电子邮件中过滤出垃圾邮件，也可以限制外部访问，使外部用户只能访问本地 Web 服务器中的某些信息。

3）安全日志功能

防火墙可以完整地记录网络通信情况，包括哪个用户在什么时间进行了什么操作，通过分析日志文件，可以发现潜在的威胁，并及时调整安全策略进行防范。一旦网络发生了入侵或遭受到了破坏，通过分析审计日志文件就可以发现线索。

4）集中管理功能

防火墙需要针对不同的网络情况和安全需求，制定不同的安全策略，并且还要根据情况的变化调整安全策略，然后在防火墙上实施。由于在一个网络的安全防护体系中，可能会有多台防火墙同时部署，所以防火墙需要进行集中管理，方便实施统一的安全策略，避免出现配置上的安全漏洞。

5）其它附加功能

除了上述的基本功能之外，防火墙一般还具有如下的附加功能：

（1）流量控制功能。针对不同的用户限制不同的流量，便于合理使用网络带宽。

（2）NAT（网络地址转换）功能。实现内部网络 IP 地址向外部网络 IP 地址的转换，可以节省外部网络 IP 地址的使用，也可以实现内部网络 IP 地址的保护，避免遭受外部网络的攻击。

（3）VPN（虚拟专用网）功能。通过利用数据封装和数据加密技术，使本来只能在私有网络传输的数据能够通过公共网络（如互联网）进行传输，大大降低了所需费用。由于防火墙所处的位置在网络的入口处，因此它是支持 VPN 连接的理想接点。

3．防火墙的分类

根据实现技术的不同，防火墙可以分为包过滤防火墙、状态检测防火墙和代理服务防火墙等。根据形态的不同，防火墙可分为软件防火墙和硬件防火墙。软件防火墙是运行在通用计算机操作系统之上的应用软件，该软件具有防火墙所要求的各项功能，如运行在 Windows 操作系统之上的 Windows 防火墙、运行在 Linux 操作系统之上的 iptables 开源防火墙等。硬件防火墙则是针对防火墙的特殊要求，对硬件、操作系统进行了裁减，设计、开发了防火墙专用的硬件和操作系统平台，在此平台之上运行防火墙软件。

4．防火墙的局限性

综上所述，防火墙能在网络边界对被保护网络进行很好的防护，但并不能解决所有的安

全问题，它有许多防范不到的地方，主要包括：

（1）不能防范被保护网络内部人员发起的攻击。内部人员发起的攻击，由于没有经过防火墙，所以防火墙无法提供防护。

（2）不能防范不经过防火墙的攻击。例如，在一个被保护的内部网络上存在一个不受限制的拨出连接，内部网络上的用户通过 ADSL 直接连接到互联网，从而绕过防火墙提供的安全系统，造成了一个潜在的后门攻击通道。

（3）不能完全防止传送已感染病毒的软件或文件。这是因为病毒的类型太多，不同操作系统的编码和压缩二进制文件的格式也各不相同，所以不能期望防火墙能对每一个进出内部网络的文件进行扫描，查出潜在的病毒。

（4）不能防范数据驱动型攻击。数据驱动型攻击从表面上看是无害的数据通过电子邮件发送或其它方式复制到内部网络主机上，但一旦被执行就形成攻击。例如，一个数据驱动型攻击可能导致主机修改与安全相关的文件，使得入侵者很容易获得对系统的访问权。

（5）不能防范不断更新的攻击方式。防火墙是一种被动式的防护手段，设置的安全策略只能对现在已知的网络威胁起作用。随着网络攻击手段的不断更新和一些新的网络应用的出现，不可能靠一次性的防火墙设置来解决永远的网络安全问题。

2.5.2 入侵检测系统

1．概述

上节介绍的防火墙是目前应用最为广泛的安全设备之一，能够有效地阻止外部网络的入侵，是对内部网络进行保护的第一道屏障。然而，如果入侵者成功地绕过了防火墙，渗透到内部网络中，如何检测出攻击行为呢？而且，对于内部人员发起的攻击，防火墙也是无能为力的，而统计结果显示，绝大多数的攻击都是由内部人员引起的。在此，本小节介绍另外一种常用的安全设备——入侵检测系统（Intrusion Detection System，IDS）。IDS 通过监视受保护系统或网络的状态，可以发现正在进行或已发生的攻击。

2．入侵检测系统的功能

一个入侵检测系统一般包括以下功能：

（1）监视用户和系统的活动。入侵检测系统通过获取进出某台主机的数据、某个网段的数据、或者通过查看主机日志信息等监视用户和系统的活动。

（2）发现入侵行为。这是入侵检测系统的核心功能，主要包括两个方面：一方面是通过分析用户和系统的活动，判断是否存在对系统的入侵行为；另一方面是评估系统关键资源和数据文件的完整性，判断系统是否已经到入侵。前者的作用是在入侵行为发生时及时发现，从而避免系统遭受到攻击；后者一般是系统在遭到入侵时没能及时发现，攻击的行为已经发生，但可以通过攻击行为留下的痕迹了解攻击情况，从而避免再次遭受攻击。对系统资源完整性的检查也有利于对攻击者进行追踪和对攻击行为的取证。对入侵行为的判断包括异常检测和误用检测两种方法。现在的入侵检测产品主要使用基于模式匹配的误用检测技术。

（3）记录和报警。入侵检测系统在检测到入侵行为后，记录入侵行为的基本情况，并采取相应的措施及时发出报警。某些入侵检测系统能够实现与防火墙等安全部件的联动。

3．入侵检测系统的分类

根据入侵检测数据的来源不同，可以分为基于主机的入侵检测系统和基于网络的入侵检测系统。

1）基于主机的入侵检测系统

基于主机的入侵检测系统主要用于保护运行关键应用的主机。它通过监视与分析主机的审计记录和日志文件来检测入侵。日志中包含发生在系统上的不寻常和不期望活动的证据，这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件，能够发现入侵企图或成功的入侵。

基于主机入侵检测系统的优点包括：（1）能确定攻击是否成功。主机是攻击的目的所在，所以基于主机的入侵检测系统使用含有已发生的事件信息，能够判断攻击是否成功。（2）监视粒度更细。可以很容易地监视系统的一些活动，如对敏感文件、目录、程序或端口的存取。（3）配置灵活。用户可根据每一台主机上的入侵检测系统实际情况进行配置。（4）可用于加密和交换的网络环境。（5）对网络流量不敏感。（6）不需要额外的硬件。

基于主机的入侵检测系统的主要缺点是：它会占用主机的资源，在主机上产生额外的负载；与主机平台相关，可移植性差；另外，操作系统的脆弱性能够破坏基于主机的入侵检测系统的完整性。

2）基于网络的入侵检测系统

基于网络的入侵检测系统主要用于实时监测网络关键路径的信息，侦听网络上的所有分组来分析入侵行为。

基于网络的入侵检测系统有以下优点：（1）实时机制提供了网络基础设施的足够保护；（2）可以检测面向网络的攻击；（3）从性能和可靠性观点来看，网络级传感器的插入并不会影响已有的网络性能；（4）合理配置的网络传感器可以在管理控制台提供全面的企业级视图，从而发现任何大规模的攻击；（5）操作员只需要对单一的网络入侵检测系统平台进行练习和培训。

基于网络的入侵检测系统的主要缺点是：难于在现代交换网络环境下进行部署，网络入侵检测系统必须在每一网络分段使用，因为它们无法跨越路由器和交换机进行监测；无法在加密的网络环境下使用，因为网络流量被加密后，网络传感器无法对数据包的协议或内容进行分析。

4．入侵检测系统的局限性

入侵检测系统不具有访问控制的能力，它通过对数据包流的分析，从数据流中过滤出可疑数据包，通过与已知的入侵方式进行比较，确定入侵是否发生以及入侵的类型并进行报警。网络管理员然后将根据报警信息确切了解所遭受的攻击并采取相应的措施。

入侵检测系统的单独使用不能起到保护网络的作用，也不能独立地阻止任何一种攻击。它在网络安全系统中所充当的角色是侦察和预警功能，协助网络管理员发现并处理已知的入侵。

由于入侵检测系统对攻击行为不能直接自动处理，而入侵检测系统和防火墙的联动也因为不同厂商的合作问题没有取得很好的效果，近年来出现了 IPS（入侵防御系统）的概念和产品。与入侵检测系统不同，入侵防御系统是串接在网络上，能够丢弃所发现的攻击数据包，只允许其它正常通信流量通过。但是，因为入侵防御系统的阻断行为对网络影响极大，不容有失，但其还没有解决入侵检测系统在漏报率、误报率方面的问题，目前入侵防御技术的发展比较缓慢。

2.5.3 恶意代码防护

1．概述

恶意代码就是一个计算机程序或一段程序代码，可以被执行完成特定的功能，但与正常的计算机软件功能不同，它是有恶意的，即起着破坏性的作用，例如计算机病毒就是最常见的一类恶意代码。

随着软件应用越来越复杂，软件中的“臭虫（bug）”和安全漏洞通常被能够写出恶意代码的用户所知晓。由于个人计算机的广泛应用以及缺乏有效的恶意代码防护机制，编写者就能够相对容易地写出恶意代码，并且欺骗毫无察觉的用户去复制和下载。随着互联网的迅速发展和广泛应用，进一步加速了恶意代码的传播，使得目前计算环境中的新恶意代码的数量呈指数级增长。

通过恶意代码防护技术，可以检测和删除网络或系统中的恶意代码，确保授权的用户、

管理员能够通过一种安全的方式执行日常任务。

2．恶意代码分类

恶意代码一般分为病毒、蠕虫、特洛伊木马和逻辑炸弹等类型，下面对每一种类型进行简单的介绍。

1）病毒

计算机病毒最早是由美国计算机病毒研究专家 Fred Cohen 博士正式提出来的，他对计算机病毒下的定义是：“病毒是一种靠修改其它程序来插入或进行自身拷贝，从而感染其它程序的一段程序。”这一定义作为标准已被广泛接受。计算机病毒具有传染性、隐蔽性、潜伏性、多态性和破坏性等特征。

从恶意代码的角度来说，根据病毒危害程度的大小不同，可以分为：无大害的病毒、数据更改型病毒和灾难性病毒。

（1）无大害的病毒。驻留在系统的不敏感区域，不会导致太大的破坏。主要感染与系统有关的磁盘或其它介质，但其目的不是破坏，经常是病毒制造者对其技术水平的一种炫耀。

（2）数据更改型病毒。能够更改系统数据，如更改电子表格、数据库系统和其它应用程序数据文件中的数据，例如把所有出现的数字 6 改成数字 9 等。

（3）灾难性病毒。可能删除关键的系统文件，并能立即导致大范围的破坏。

2）蠕虫

蠕虫主要是指利用操作系统和应用程序漏洞传播，通过网络通信功能将自身从一个结点发送到另一个结点并启动运行的程序。它可以算是计算机病毒中的一种，但与普通计算机病毒之间有着很大的区别。它具有计算机病毒的一些共性，如传播性、隐蔽性、破坏性等等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），对网络造成拒绝服务，以及与黑客技术相结合等等。

在破坏性上，蠕虫病毒也不是普通病毒所能比拟的，互联网使得蠕虫可以在短短的时间内蔓延全球，造成网络瘫痪。局域网条件下的共享文件夹、电子邮件、大量存在漏洞的服务器等，都成为蠕虫传播的良好途径。此外，蠕虫会消耗内存或网络带宽，从而可能造成拒绝服务，导致计算机崩溃。

3）特洛伊木马

木马是因希腊神话里面的“特洛伊木马”得名的，指一个隐藏在合法程序中的非法的程序。该非法程序被用户在不知情的情况下执行。当有用程序被调用时，隐藏的木马程序将执行某种有害功能，例如删除文件、发送信息等，并能用于间接实现非授权用户不能直接实现的功能。木马不会感染其它寄宿文件，清除木马的方法是直接删除受感染的程序。

木马与病毒的重大区别是木马不具传染性，它并不能像病毒那样复制自身，也并不“刻意”地去感染其它文件，它主要通过将自身伪装起来，吸引用户下载执行。要使木马传播，必须在计算机上有效地启用这些程序，例如打开电子邮件附件或者将木马捆绑在软件中放到网络吸引人下载执行等。

现在常见木马主要以窃取用户相关信息为主要目的，它主要由两部分组成：服务器程序和控制器程序。感染木马后，计算机中便安装了服务器程序，拥有控制器程序的人就可以通过网络远程控制受害者的计算机，为所欲为。

4）逻辑炸弹

逻辑炸弹可以理解为在特定逻辑条件满足时实施破坏的计算机程序。与病毒相比，逻辑炸弹强调破坏作用本身，而实施破坏的程序不会传播。

逻辑炸弹在软件中出现的频率相对较低，原因主要有两个：首先逻辑炸弹不便于隐藏，可以追根朔源；第二，相当多的情况下，逻辑炸弹在民用产品中的应用是没有必要的，因为这种手段“损人不利己”，而在军用或特殊领域，如国际武器交易、先进的超级计算设备出

口等情况下，逻辑炸弹才具有实用意义，如逻辑炸弹可以限制超级计算设备的计算性能或使得武器的电子控制系统通过特殊通信手段传送情报或删除信息等。

值得注意的是，近年来在民用场合也确实发生过多起逻辑炸弹引发的信息安全事件，原因是有的单位员工出于对单位不满而在为客户开发的软件中设置逻辑炸弹，导致客户的信息系统在运行一段时间后出现重大故障，甚至造成严重经济损失。

3．恶意代码处置

恶意代码检测包括三个阶段，首先用户检测到恶意代码的存在，其次对存在的恶意代码做出反应，最后在可能的情况下恢复数据或系统文件。

1）检测阶段

检测阶段的目的是发现恶意代码存在和攻击的事实。传统的检测技术一般都采用“特征码”检测技术，即当发现一种新的病毒或蠕虫、木马后，采集其样本，分析其代码，提取其特征码，然后加入到特征库中去，进行扫描时即是与库内的特征码去匹配，匹配成功，则报告发现恶意代码。目前的反病毒软件都能检测一定数量的病毒、蠕虫和特洛伊木马。

但是特征码检测技术有着致命的弱点，即它只能检测已知的恶意代码，当新的恶意代码出现时，它是无能为力的。因而，当前人们研究的热点是如何预防和检测新的、未知的恶意代码，例如启发式检测法、基于行为的检测法等。

2）反应阶段

若在网络或系统内已经检测到恶意代码的存在，则对恶意代码做出反应。包括定位恶意代码的存储位置、辨别具体的恶意代码、删除存在的恶意代码并纠正恶意代码造成的后果等。

3）恢复阶段

一旦网络或系统内的文件、数据或系统本身遭受了恶意代码感染，除了清除恶意代码外，还需要通过对有关恶意代码或行为的分析结果，找出事件根源并彻底清除。此外，还应把所有被攻破的系统和网络设备彻底还原到它们正常的任务状态，并恢复被破坏的数据。

本章小结

本章介绍了以下信息安全基础知识，这些知识大都侧重于体系结构，旨在为进一步掌握信息安全知识体系奠定基础：

（1）信息系统安全要素

信息系统安全保护的实质是风险管理，信息系统安全保护的直接目的便是控制安全风险。“风险”及其相关概念构成了影响信息系统安全的主要因素，它们不但揭示了信息安全问题产生的原因，也因此导出了信息安全问题的解决方案。

信息系统的脆弱性是安全风险产生的内因，威胁则是安全风险产生的外因，威胁要利用脆弱性才能够造成安全风险。信息安全保护的实质，就是在综合考虑成本与效益的前提下，通过安全措施来控制风险，使残余风险降低到可接受的程度。由于任何信息系统都会有安全风险，人们追求的所谓安全的信息系统，实际是指信息系统在实施了风险评估并做出风险控制后，仍然存在的残余风险可被接受的信息系统。因此，不存在绝对安全的信息系统（即“零”风险的信息系统），也不必要追求绝对安全的信息系统。

常见的风险控制措施有四种：风险降低、风险承受、风险规避和风险转移。只有威胁和脆弱性的共同作用才会产生风险。而如果脆弱性不能被利用，或者攻击者的攻击成本大于获利，则都不会造成风险。因此，风险控制的实施点和具体的风险控制措施与风险评估的结果密切相关。

（2）网络安全基础

OSI 参考模型按功能划分为 7 个层次，从低到高依次为：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。它从概念和功能上给出了一种异型网络互连的标准框架，

是开发网络协议标准和体系结构的理论框架。但由于其结构复杂，OSI 参考模型从来没有真正意义上实现过。

TCP/IP 协议族由 5 层构成，从低到高依次为：物理层、数据链路层、网络层、传输层和应用层。目前，它已成为事实上的国际标准和公认的工业标准。

开放系统互联安全体系结构是基于 OSI 参考模型的 7 层协议之上的一种网络安全体系结构。该标准的核心内容是，为了保证异构计算机进程之间远距离交换信息的安全，定义了系统应当提供的 5 类安全服务和 8 种安全机制，确定了安全服务与安全机制之间的关系以及在 OSI 参考模型中安全服务和安全机制的配置，另外还确定了 OSI 的安全管理。必须指出，开放系统互联安全体系结构只是 ISO 参考模型框架下的一种网络安全体系结构，并不能将其视为信息安全的体系结构。其“安全服务”概念的来源，便是因为 OSI 七个层中每一层对其上一层的功能支持称为“服务”。显然，开放系统互联安全体系结构所提出的 5 类安全服务和 8 种安全机制仅仅属于通信安全的范畴，且侧重于在 OSI 七层协议上的分解。这个体系结构不能完整描述信息安全的需求和技术组织架构。

（3）信息安全保障体系

信息安全保障体系是指实施信息安全保障的法制、组织管理和技术等层面有机结合的整体，是信息社会国家安全的基本组成部分，是保证国家信息化顺利进行的基础。它不但是国家信息安全保障工作的着眼点，也是国家信息安全保障能力的载体。

国家信息安全保障体系的目标是确保基础信息网络和重要信息系统的安全，创建安全健康的网络环境，其内容是建设信息安全法制体系、信息安全组织管理体系、信息安全技术保障体系、信息安全平台及基础设施，并提供信息安全经费保障体系和信息安全人才保障体系这两个支撑条件。

（4）积极防御的信息安全技术保护框架

当前大部分信息安全系统主要是由防火墙、入侵检测、病毒防范等组成，这种以“老三样”为主要手段的这类信息安全保护思路已经越来越显示出被动性，迫切标本兼治的新型的信息安全保护框架。

现在的 PC（个人计算机）机软、硬件结构简化，导致资源可任意使用，尤其是执行代码可修改，恶意程序可以被植入。因此，终端不安全是问题的核心所在。积极防御的基本思路是主动防止非授权访问操作，从客户端操作平台实施高等级防范，使不安全因素从终端源头被控制。这在工作流程相对固定的重要信息系统中显得更为重要而可行。为此，以可信的应用操作平台为核心，辅以安全的共享服务资源边界保护、全程安全保护的网络通信和安全管理中心，便构成了工作流程相对固定的生产系统的信息安全保护框架。

（5）常用安全技术

本章对防火墙、入侵检测系统和恶意代码防护技术进行了概念层次的介绍，包括各项技术的分类及功能优缺点。这些技术及产品并不是本书的重点，仅作为常识材料提供给读者。

习题

1．概述信息系统安全要素，并说明各要素之间的关系。
2．画出 OSI 参考模型的层次结构图，并概述各层的主要功能。
3．画出 TCP/IP 模型的层次结构图，并概述各层的主要功能。
4．OSI 开放系统互连安全体系中包含哪些安全服务？
5．OSI 开放系统互连安全体系中包含哪些安全机制？
6．概述安全服务和安全机制的关系。
7．信息安全保障体系由哪些部分组成？
8．传统的信息安全保护思路存在哪些弊端？

9．概述积极防御的信息安全技术保护框架的主要内容。
10．“两个中心”支持下的三重信息安全技术保护框架与 OSI 开发系统互联安全体系结构的区别是什么？
11．概述防火墙的作用、分类及主要功能。
12．概述入侵检测系统的作用、分类及主要功能？
13．恶意代码可以分为哪些常见类型？

第 3 章　密码技术与应用

本章要点

- 密码学基本概念
- DES 算法
- RSA 算法
- MD5 算法
- SHA-1 算法
- 数字签名

3.1　密码技术概述

密码学是以研究秘密通信为目的而产生的学科。它的研究内容之一是对传输信息采用何种秘密的变换，才能防止攻击者对截取传输信息后的还原。密码学分为两个相对独立的分支，密码编码学和密码分析学。密码编码学的主要目的是寻求保证信息保密性或可认证性的方法，密码分析学的主要目的是研究加密信息的破译或信息的伪造。

为了隐藏和保护要发送的信息，使未授权者不能提取信息，通信双方要采用保密通讯系统。发送方把要发送的信息即明文，在发送前利用加密算法将它变换成看似无意义的随机信息即密文。接收方对接收到的密文利用解密算法进行解密。

3.1.1　基本概念

采用密码技术可以隐藏和加密需要保护的信息，使未授权者不能提取原始的信息。被加密的原始信息称为明文，加密后的信息称为密文。将明文变换为密文的过程称为加密（Encryption），其逆过程，即将密文变换为明文的过程称为解密（Decryption），对明文进行加密操作的人员称作加密员或密码员（Cryptographer）。密码员对明文进行加密操作时所采用的一组规则称作加密算法（Encryption Algorithm）。所传送信息的预定对象称为接收者（Receiver）。接收者对密文解密所采用的一组规则称为解密算法（Decryption Algorithm）。加密和解密算法的操作通常都是在一组密钥的控制下进行的，分别称为加密密钥（Encryption Key）和解密密钥（Decryption Key）。因为数据以密文的形式存储于计算机文件中，或在数据通信网络中传输，因此即使数据被未授权者非法窃取，未授权者也不能理解其真实含义，从而达到数据保密的目的。同样，未授权者也不能伪造合理的密文，因而不能篡改数据，以此达到确保数据真实性的目的。

一个密码系统通常由五个部分组成：

（1）明文空间 M，它是全体明文的集合。

（2）密文空间 C，它是全体密文的集合。

（3）密钥空间 K，它是全体密钥的集合，其中每一个密钥 K，均由加密密钥 K_e 和解密密钥 K_d 组成，即 $K=(K_e, K_d)$。

（4）加密算法 E，由加密密钥控制的加密变换的集合。

（5）解密算法 D，由解密密钥控制的解密变换的集合。

设 $m \in M$，对于确定的密钥 $K=(K_e, K_d)$，则

$$c = E_{Ke}(m) \in C,$$

$$m = D_{Kd}（c） \in M,$$

其中 E_{Ke} 是由加密密钥 K_e 确定的加密变换，D_{Kd} 是由解密密钥 K_d 确定的解密变换，并且在一个密码体制中，要求解密变换是加密变换的逆变换。因此对任意的 $m \in M$，都有：

$$D_{Kd}（E_{Ke}（m））= m$$

成立。

3.1.2 密码学的发展历史

密码学的发展大致可以分为三个阶段：

第一个阶段是从几千年前到 1949 年。这一时期的可以看作是科学密码学的前夜，这段时期的密码技术与其说是一种科学，不如说是一种艺术。密码学专家常常是凭自己的直觉和信念来进行密码设计，而对密码的分析也多基于密码分析者（也就是破译者或攻击者）的直觉和经验。

第二个阶段是从 1949 年到 1975 年。1949 年 Shannon（香农）发表的《保密系统的信息理论》一文标志着密码学的这一阶段的开始。Shannon 的这篇文章产生了信息论，为私钥密码系统建立了理论基础，从此密码学成为一门科学。但科学理论的产生并没有使密码学丧失艺术的一面，一直到今天，密码学仍是一门非常艺术性的科学。

这两个阶段的密码，是平常人们接触不到的密码。出于保密，人们基本上看不到关于密码学的文献和资料。1967 年 Kahn 出版了一本叫做《破译者》的书（可以说这本书是一本小说），才使看到书的人们惊讶到：原来还有密码学这样一个领域！但这本书只是讲述一段值得注意的完整的经历，也部分涉及了一些当时仍旧保密的事情。70 年代初期，IBM 发表了有关密码学的几篇技术报告，使更多的人了解到了密码学的存在。

第三阶段为 1976 年至今。1976 年 Diffe 和 Hellman 发表了《密码学新方向》一文，导致了密码学发展史上的一场革命。这篇论文首次证明了在发端和收端不需要传输密钥的保密通信的可能性，从而开创了公钥密码学的新纪元。也从此，密码才开始充分发挥它的商用价值和社会价值，普通大众才能够接触到密码学并从中受益。

3.1.3 密码体制分类

根据密码体制所使用的密钥，可以将其分为两类，即单钥密码体制与双钥密码体制。

单钥密码体制又称对称密码体制，加密和解密均采用同一密钥，而且通信双方都必须获得这一密钥。它的安全性依赖以下两个因素。第一，加密算法必须是足够强的，仅仅基于密文本身去解密信息在计算上是不可能的；第二，加密方法的安全性根本上是依赖密钥的秘密性，而不仅是算法的秘密性。因此，即使算法的秘密性暴露，但由于保证了密钥的秘密性，加密的使命依然可以得到保证。这就是在现代国际密码界可以公开密码算法（如后几节谈到的 DES、AES 等），但它们仍被广泛使用的科学依据。单钥密码体制最大的问题是密钥的分发和管理非常复杂、代价高昂。例如对具有 n 个用户的网络，需要 n(n－1)/2 个密钥，在用户群不是很大的情况下，单钥体制是有效的。但是对大型网络，当用户群很大、分布很广时，密钥的分配和保存就成了大问题。

单钥密码体制对明文信息的加密有两种方式：一是明文信息按字符（如二元数字）进行逐字符加密，称之为流密码或序列密码，另一种是将信息分组（含多个字符），逐组地进行加密，称之为分组密码。

双钥密码体制又称为非对称密码体制或公钥密码体制，它使用的加密密钥（又称为公钥）和解密密钥（又称为私钥）是不同的，且加密密钥是公开的，通过加密密钥 K_e 计算解密密钥 K_d 是很困难的。因此，在公钥密码体制中密钥的分配和管理就很简单，例如对具有 n 个用户的网络，只需要 $2n$ 个密钥。在实际应用中，双钥密码体制并没有完全取代单钥密码体制，这是因为双钥密码体制是基于尖端的数学难题，计算非常复杂。但它实现速度却远不及单钥密码体制。在实际应用中可利用二者的各自优点，采用单钥密码体制加密文件，采用双

钥密码体制加密“加密文件”的密钥（会话密钥），这就是混合加密系统，它较好地解决了运算速度问题和密钥分配管理问题。因此，双钥密码体制通常被用来加密关键性的、核心的保密数据，而单钥密码体制通常被用来加密大量的明文数据。

3.1.4 密码攻击概述

密码分析学的主要目的就是在不知道密钥的情况下，恢复出明文。成功的密码分析能恢复出密文所对应的明文或加密所使用的密钥，并且密码分析也可以发现密码系统的弱点，为达到最终掌握算法及密钥的目的提供知识。

1．攻击方法

对密码进行分析的尝试称为攻击。攻击方法主要有以下三种：

1）穷举攻击

所谓穷举攻击就是密码分析者用使遍所有密钥的方法来破译密码。穷举攻击所花费的时间等于尝试次数乘以一次解密（加密）所需的时间。显然可以通过增大密钥量或加大解密（加密）算法的复杂度来对抗穷举攻击。现代密码体制往往经过了精心设计，这种攻击方法一般不会有什么效果。

2）统计分析攻击

所谓统计分析攻击是指密码分析者通过分析明文与密文的统计规律来破译密码。统计分析攻击在历史上为破译密码做出过很大的贡献。对抗统计分析攻击的方法就是设法使明文的统计特性不带入密文，也就是明文的统计特性与密文的统计特性不一样。

3）数学分析攻击

密码分析者针对加密算法的数学基础，通过数学求解的方法来破译密码。为对抗这种攻击应选用具有坚实的数学基础和足够复杂的加密算法。

2．攻击分类

根据密码分析者可利用的数据来分类，可将攻击分为以下几类，当然每一类都假设密码分析者知道所用的加密算法的全部知识：

1）唯密文攻击

密码分析者有一些信息的密文，这些信息都用同一加密算法加密。密码分析者的任务是恢复尽可能多的明文，或者最好是能推算出加密信息的密钥来，以便可采用相同的密钥解出其它被加密的信息。

2）已知明文攻击

密码分析者不仅可得到一些信息的密文，而且也知道这些信息的明文。分析者的任务就是用加密信息推出用来加密的密钥或导出一个算法，此算法可以对用同一密钥加密的任何新的信息进行解密。

3）选择明文攻击

分析者不仅可得到一些信息的密文和相应的明文，而且他们也可选择被加密的明文。这比已知明文攻击更有效。因为密码分析者能选择特定的明文块去加密，那些块可能产生更多关于密钥的信息。分析者的任务是推出用来加密信息的密钥或导出一个算法，此算法可以对用同一密钥加密的任何新的信息进行解密。

4）选择密文攻击

在选择密文攻击中，密码分析者能选择不同的被加密的密文，并可得到对应的明文。

除了上面介绍的几种攻击方法外，还有其它的攻击方法，在此不一一介绍，感兴趣的读者可参考有关文献。

3.1.5 保密通信系统

基于前面的知识，我们来看一下保密通信系统。在信息传输与处理系统中，除了意定的接收者外，还有非授权者，他们通过各种方法来窃取保密信息，这类非授权者被称为截收者或攻击者。截收者虽不知道解密密钥，但通过分析可能从截获的密文中推断出明文或解密密钥，这种攻击是被动攻击。另一种攻击则是主动攻击，即非法入侵者或攻击者主动向系统窜扰，采用删除、添加、伪造、重放等手段向系统注入假信息，以达到自己的目的。

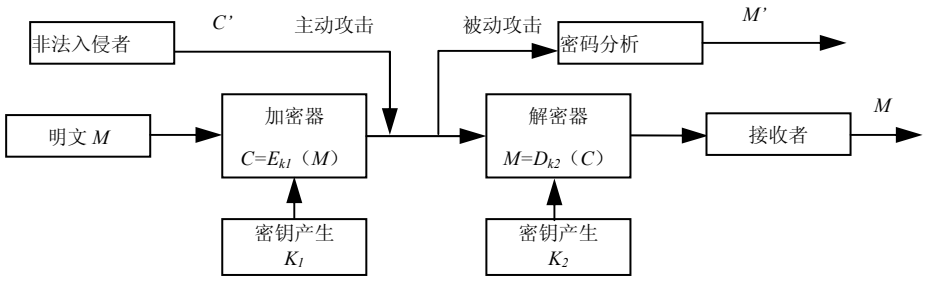


图 3-1　保密通信系统模型

保密通信系统可用图 3-1 表示，它由以下几部分组成：明文信息空间 M，密文信息空间 C，加密密钥空间 $K1$ 和解密密钥空间 $K2$。在单钥密码钥体制下，$K1 = K2 = K$, 此时密钥 K 需通过安全信道由发送方传给接收方。加密变换 E_{k1} ：$M \rightarrow C$，$k1 \in K1$，由加密器完成；解密变换 D_{k2} ：$C \rightarrow M$，$k2 \in K2$，由解密器完成。对每一个密钥 $k1 \in K1$（$k1$ 确定一个加密变换 E_{k1}），都有一个对应的 $k2 \in K2$（$k2$ 确定一个加密变换 D_{k2}），使得对任意 $m \in M$，都有

$$D_{K2}（E_{K1}（m））= m$$

为了保护信息的保密性，保密通信系统应当满足如下要求：

（1）系统即使达不到理论上的不可破解，即系统无法使 $m' = m$ 的概率为 0，也应当是实际上不可破解的，即计算上是不可行的。

（2）系统的保密性不能依赖对加密算法的保密，而依赖于密钥。

（3）加密与解密算法适用于所有密钥空间中的元素。

（4）从截获的密文或已知的密文明文对，推断密钥或任意明文在计算上是不可行的。

为了防止信息被删除、添加、伪造、重放等，一种有效的方法就是使发送的信息具有被验证的能力，使接受者能够识别和确认信息的真伪，具有这类功能的保密系统称之为认证系统。信息的真实性与信息的保密性不同，信息的保密性是使截获者在不知道密钥的条件下不能解读密文的内容，而信息的真实性是使任何不知道密钥的人不能构造出一个密文，使意定的接收者解密成一个可理解的合法信息。

3.2　流密码

流密码又称为序列密码，是密码学的一个重要分支，目前对它的研究比较成熟。由于它具有速度快、实现简单等特点，广泛应用于军事等各个领域。

3.2.1　基本原理

流密码的基本思想是对明文符号序列

$$m = m_0 m_1 \ldots\ldots$$

用密钥流

$$z = z_0 z_1 \ldots\ldots$$

按如下的规则进行加密产生密文符号序列：

$$y = y_0 y_1 \ldots\ldots = Ez_0（m_0）Ez_1（m_1）\ldots\ldots$$

流密码的安全性主要依赖于密钥流。对于一个流密码，如果存在一个固定的 T，使得密钥流每隔 T 个密钥符号后就出现重复，则称该流密码是周期的；否则，流密码称为非周期的。如果密钥流是完全随机的密钥符号序列，则对应的流密码是“一次一密”的。因为产生

一个完全随机的密钥流的方法，很难重复产生相同的密钥流，所以我们必须在信息的发送方与接收方之间通过秘密通道来传递密钥流，通常明文符号序列很长，同时也决定了密钥流很长，这么长的密钥流会在存储与分发等方面产生诸多不利。尽管 Shannon 证明了“一次一密”密码体制是安全的，是不可破的，不过这种密码意义不大，在实际应用中，一般是利用一个短的种子密钥 k 来产生一个很长的密钥流，并且把密钥流的每个密钥符号 z_i 看作是种子密钥 k 和流密码在时刻 i 的内部状态 σ_i 的函数，即 $z_i = f(k, \sigma_i)$，$i = 0, 1, \ldots\ldots$。这样生成的密钥流，并不是完全随机的，而是伪随机的。人们一般提到流密码就是指基于这种密钥流的。但为了流密码的安全，要求这样的伪随机要满足一定的特性，如：

（1）极大的周期；

（2）良好的统计特性；

（3）线性不可预测性要充分大。

3.2.2 流密码分类

在流密码中，有两种不同的加密方式，即同步方式和自同步方式。

1．同步流密码

在同步流密码中，密钥流 $\{z_j = f(k, \sigma_j) \mid j \geq 0\}$，与明文符号无关，并且 j 时刻输出的密文也与 j 时刻之前的明文符号无关。这样可将同步密码流加密器划分为密钥流生成器和加密变换器两部分。

在同步密码流中，只要发送方与接收方有相同的种子密钥 K 和内部状态，就能产生出相同的密钥流。此时，我们说发送方与接收方的密钥生成器是同步的。一旦双方不同步，解密工作会立即失败，密码系统在这时要能提供某种手段以重建同步。图 3-2 是同步流密码模型。

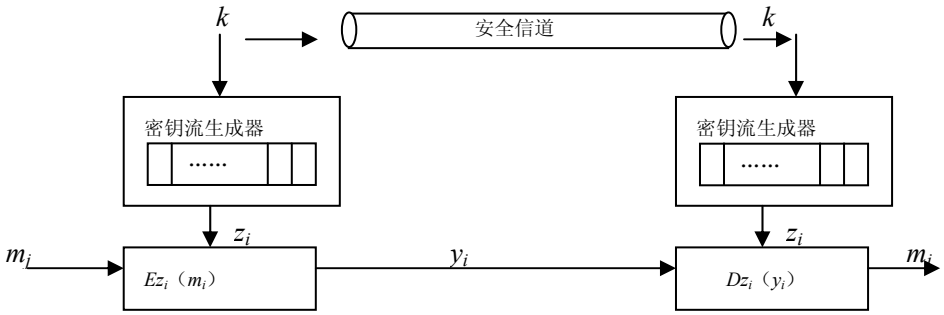


图 3-2　同步流密码模型

2．自同步流密码

在自同步流密码中，密钥流 $\{z_j = f(k, \sigma_j) \mid j=1,2,\ldots,\infty\}$，是由前面 n 个密文符号推导出来的，与明文符号有关，这样 j 时刻输出的密文符号 y_j 也不仅仅依赖于明文符号 m_j。自同步流密码常用的工作模式为密码反馈模式（见图 3-3）。在反馈工作模式中，每个密文符号 y_j 在生成之后，立即送到移位寄存器 R 的一端（另一端的符号被丢掉）。在每次迭代中，R 的值作为 E_B 的输入，输出的最低符号位作为下一个密钥符号。

对于反馈工作模式，传输错误将影响反馈圈。如果一个密文符号在传输中出错或丢失，要等到该错误移出寄存器才能同步。

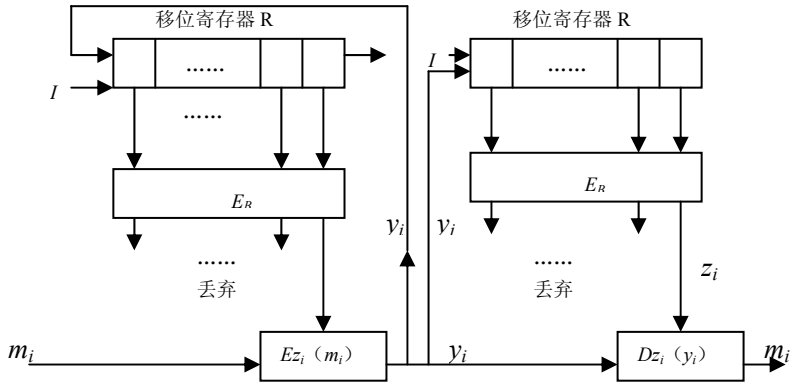


图 3-3　自同步流密码的密码反馈模式

3.2.3　密钥流生成器

从公开发表的文献来看，目前绝大多数有关流密码的研究成果都是关于同步流密码的。一个同步流密码是否具有很高的密码强度主要取决于密钥流生成器，因此这里介绍同步流密码的密钥流生成问题。

一般来说，可以将同步流密码密钥流生成器看作成一个参数为 k 的有限状态自动机，它由一个输出符号集 A，一个状态集 S，一个状态转移函数 f，一个输出函数 g 以及一个初始状态 σ_0 组成，如图 3-4 所示。状态转移函数 f：$\sigma_i \rightarrow \sigma_{i+1}$，将当前状态变为一个新的状态。输出函数 g: $\sigma_i \rightarrow z_i$，将当前状态变为输出符号集 A 中一个元素 z_i 。因此，这种密钥流生成器设计的关键在于找出适当的状态转移函数 f 和输出函数 g，使得输出序列 $z = z_0 z_1 \ldots$ 满足需要。一般来说状态转移函数 f 和输出函数 g 应为非线性函数，但这里取状态转移函数 f 是线性，输出函数 g 为非线性的。为了便于从理论上对这类生成器进行分析，可将其分成驱动部分和非线性组合部分。驱动部分控制生成器的状态转移，并为非线性组合部分提供统计性能良好的序列，如驱动部分是由一组线性反馈移位寄存器构成；而非线性组合部分充分利用这些序列，组合出满足条件的密钥流序列，如图 3-5 所示，图中 Si（$i=1,2, \ldots,n$)是线性反馈移位寄存器 i 输出的序列。

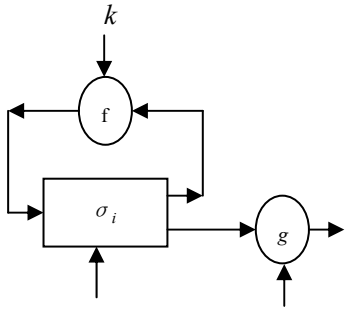


图 3-4　作为有限自动机的密钥流生成器

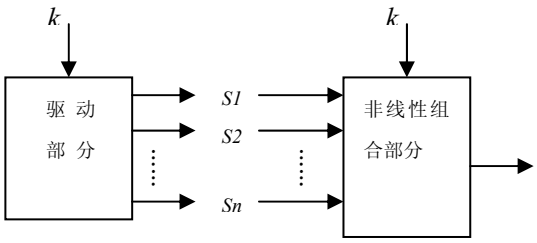


图 3-5　密钥流生成器的分解

线性反馈移位寄存器 LFSR（linear feedback shift register）是构造密钥流生成器的重要部件之一，并且因其实现简单、速度高、便于分析等特点而广泛应用于数字电路中。限于篇幅，这里就不再介绍，感兴趣的读者可以参考有关文献。

3.3　分组密码

分组密码是将明文信息编码表示后的数字序列 $x_0,x_1,\ldots,x_i,\ldots$ 划分成长为 n 的组 $x=(x_0, x_1,\ldots,x_{n-1})$，各组（长为 n 的矢量）分别在密钥 $k=(k_0,k_1,\ldots,k_{t-1})$ 的控制下，变换成输出序列 $y=(y_0,y_1,\ldots,y_{m-1})$（长为 m 的矢量），其加密函数为 $E:Vn\times K\rightarrow Vm$，解密函数为 $D:Vm\times K\rightarrow Vn$，$Vn$ 和 Vm 分别是 n 维和 m 维矢量空间，K 为密钥空间，如图 3-6 所示。若 $m>n$，则为有数据扩展的分组密码；若 $m<n$，则为有数据压缩的分组密码；若 $m=n$，则分组密码对密文加

密后既无数据扩展也无数据压缩。

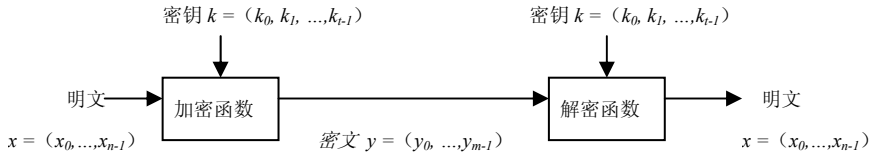


图 3-6　分组密码框架

分组密码的特点是加密密钥与解密密钥相同，分组密码的安全性应该主要依赖于密钥的保密，而不是加密算法与解密算法的保密。较早的著名的分组密码算法有 DES（数据加密标准）和 IDEA（国际数据加密算法）算法。2002 年 11 月，美国公布了旨在取代 DES 的 21 世纪的加密标准 AES（高级加密标准）算法。我国国家密码管理局在 2006 年 1 月公布了我国自主知识产权的 SMS4 密码算法，这是我国目前公布的第一个也是唯一一个密码算法。

3.3.1　概述

1．分组密码的设计原则

下面从安全性和实现两个方面介绍分组密码的设计原则。

1）针对安全性的设计原则

影响分组密码安全性的因素很多，诸如分组长度和密钥长度等，但针对安全性的两个一般设计原则是 Shannon 提出的扩散和混淆原则，这两个原则的目的就是为了抵抗对密码的统计分析。如果攻击者知道明文的某些统计特性，如消息中不同字母出现的频率、可能出现的特定单词或短语，而且这些统计特性以某种方式在密文中反映出来，那么攻击者就有可能得出加密密钥或其一部分，或者得出包含加密密钥的一个可能的密钥集合。在 Shannon 称之为理想密码的密码系统中，密文的所有统计特性都与所使用的密钥独立。

所谓扩散，就是将明文的统计特性散布到密文中去，实现方式是使得明文的每一位影响密文中多位的值，等价于说密文中每一位均受明文中多位影响。在分组密码中，可对数据重复执行某个置换，再对这一置换作用于一函数，可获得扩散。

所谓混淆，就是使密文和密钥之间的统计关系变得尽可能复杂，使得攻击者即使获取了关于密文的一些统计特性，也无法推测密钥。使用复杂的代换算法可以得到预期的混淆效果，

扩散和混淆成功地实现了分组密码的本质属性，因而成为设计现代分组密码的基础。

2）针对实现的设计原则

分组密码可以用软件和硬件来实现。硬件实现的优点可获得高速率，软件实现的特点则是灵活性强，代价低。因此，分组密码的设计可根据预定的实现方法来考虑。

软件实现的设计原则：使用子块和简单的运算。密码运算在子块上进行，因此子块的长度自然要适应软件编程，例如 8、16、32 比特等。子块上所进行的密码运算应该是易于实现的运算，最好使用一些标准处理器所具有的一些基本指令，例如加法、乘法、移位等。

硬件实现的设计原则：加密与解密可用同样的器件来实现，且尽量使用规则结构，因为密码应有一个标准的组件结构，以便能适应于大规模集成电路实现。

2．Feistel 密码结构

很多分组密码的结构从本质上说都是基于一个称为 Feistel 网络的结构，其思想实际上是 Shannon 提出的利用乘积密码实现混淆与扩散思想的具体应用。Feistel 提出利用乘积密码可获得简单的代换密码，所谓乘积密码就是指顺序地执行两个或多个基本密码系统，使得最后结果的密码强度高于每个基本密码系统产生的结果。

加密算法的输入是数据分组 M 和密钥 K。将每组明文分为左右两部分，即 L 和 R。把 L 和密钥 K 经过变换 F 得到 F_K（L）后与 R 异或，将这个过程说成是将 L 变换后异或到 R 中，并记这个运算过程为 $M'=XR_K$（M）。

记

$$M = (L,R)，M' = XRK(M) = (L',R')$$

那么

$$L' = L，R' = R \oplus FK(L)$$

上式中，“⊕”表示异或运算。图 3-7 表示了 $XR_K(M)$ 的过程。

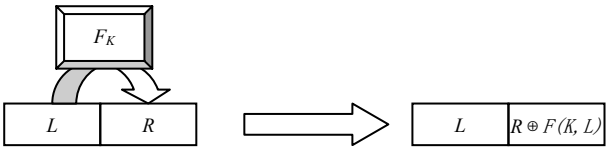


图 3-7　$XR_K(M)$ 基本过程

要从 M'反过来计算 M 应该怎么做呢？只需要将 L 经过相同变换后重新异或到 R 中就可以得到 M。从公式描述就是 $XR_K(XR_K(M)) = M$，即 XR 的逆运算就是 XR。换句话说，两次 XR 运算互相抵消。整个过程可以用图 3-8 表示。这个过程很简单，感兴趣的读者可以自行推导，这里就不再证明了。

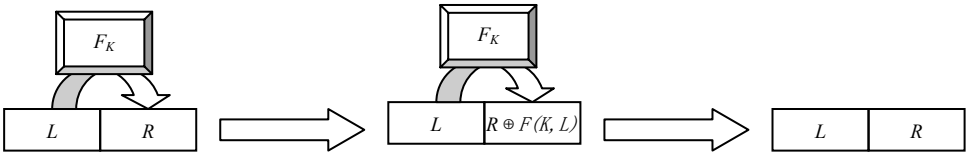


图 3-8　$XR_K(M)$ 运算

同样，也可以定义 $XL_K(M)$ 运算，也就是将数据的右半部分经过变换异或到左半部分。Feistel 密码结构就是经过多次重复的 XR 和 XL 运算实施数据的混合。在 Feistel 结构中，每轮的结构都相同，每轮中右半部分数据作用于轮函数 f 后，再与左半部分数据进行异或运算；每轮的轮函数的结构都相同，但以不同的子密钥 K_i 作为参数。每次提到的异或运算结束后，再交换左右两半部分数据。

在进行完 n 轮迭代后，左右两部分再合并到一起以产生密文分组。其中第 i 轮迭代的输入为前一轮的输出的函数：

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

其中 K_i 是第 i 轮的子密钥，由加密密钥 K 得到。一般地，各轮子密钥彼此不同而且与 K 也不同。

Feistel 网络的实现与以下参数和特性有关：

（1）组大小：分组越大安全性越高，但加密速度就越慢

（2）密钥大小：密钥越长安全性越高，但加密速度就越慢

（3）轮数：单轮结构不能保证安全性，但多轮结构可提供足够的安全性

（4）子密钥产生算法：该算法的复杂性越大，则密码分析的困难性就越大

（5）轮函数：轮函数的复杂性越大，密码分析的困难性亦越大

Feistel 解密过程本质上与加密过程是一样的，算法使用密文作为输入，但使用子密钥 K_i 的次序与加密过程相反，即第一轮使用 K_n，第二轮使用 K_{n-1}，…，最后一轮使用 K_1。这一特性保证了解密与加密采用统一算法。

3．分组密码工作模式

1）电子密码本模式（ECB）

在电子密码本（ECB）模式下，直接利用分组密码对明文的各分组分别进行加密。设明文 $M = M_0M_1...M_n$，密文 $C = C_0C_1...C_n$，其中，

$$C_i = E_k(M_i)，i=1,2,...,n$$

电子密码本模式是分组密码的基本工作模式，它的缺点就是容易暴露明文的数据模式。

2）密码分组链接（CBC）模式

在密码分组链接（CBC）模式下，每个密文块 C_i 在用密钥 K 加密下一个明文块 M_{i+1} 之前与 M_{i+1} 进行异或。正式的描述是给定一初始向量 IV，并设 $C_0=IV$，加密按下述规则进行，

$$C_i=E_k（M_i \oplus C_{i-1}）, i\geq 1$$

因此，在 CBC 模式下，即使 $M_i=M_j$，但因 $C_{i-1}\neq C_{j-1}$，也会有 $C_i\neq C_j$，这样就很好地掩盖了明文的数据模式。解密时，

$$M_i=D_k（C_i）\oplus C_{i-1}, i\geq 1$$

因此，当 C_i 中发生错误，只影响 M_i 和 M_{i+1}，不会影响其它明文块，也就说错误传播有界。

3）密文反馈（CFB）模式

密文反馈（CFB）模式工作原理是，给定一初始向量 IV，并设 $C_0=IV$，按下述规则来产生密钥流 Z_i 并进行加密，

$$Z_i=E_k（C_{i-1}）, i\geq 1$$
$$C_i=M_i \oplus Z_i, i\geq 1$$

在 CFB 模式下，即使 $M_i=M_j$，但因 $Z_i\neq Z_j$，也会有 $C_i\neq C_j$，这样就很好的掩盖了明文的数据模式。解密时有 $M_i=E_k（C_{i-1}）\oplus C_i$。因此当 C_i 中发生错误，只影响 M_i 和 M_{i+1}，不会影响其它明文块，因而象 CBC 模式一样错误传播有界。

4）输出反馈（OFB）模式

在输出反馈（OFB）模式下工作，要先产生密钥流，然后将它与明文进行异或。正式的描述是给定一初始向量 IV，并定义 $Z_0=IV$，用下述规则来产生密钥流 Z_i 和得到密文 C_i，

$$Z_i=E_k（Z_{i-1}）, i\geq 1$$
$$C_i=M_i \oplus Z_i, i\geq 1$$

输出反馈（OFB）模式的结构类似于密文反馈（CFB）模式，不同之处是：OFB 模式是将加密算法的输出反馈到移位寄存器，而 CFB 模式是将密文单元反馈到移位寄存器。OFB 模式的优点是传输过程中比特错误不会被传输；OFB 模式的缺点是它比 CFB 模式更易受到对信息流的篡改攻击。例如，在密文中取 1 比特的补，那么在恢复的明文中，相应位置的比特也为原比特的补。因此能使攻击者有可能通过对信息校验部分的篡改和对数据部分的篡改，而以纠错码不能检测的方式篡改密文。

3.3.2 DES 算法

1973 年 5 月 15 日，美国国家标准局（现在是美国国家标准与技术研究院，即 NIST），公开征集密码体制，这一举措导致了数据加密标准（DES）的出现。DES 是由美国 IBM 公司研制的，是早期的 Lucifer 密码的发展与修改。DES 在 1975 年 3 月 17 日首次被公布，1977 年 1 月 15 正式批准并作为美国联邦信息处理标准 FIPS-46，同年 7 月开始生效。当时规定每隔 5 年由美国国家安全局（NSA）做出评估，并重新批准它是否继续作为联邦加密标准。DES 的最后一次评估在 2001 年 1 月。2002 年 11 月，美国公布了旨在取代 DES 的 AES（高级加密标准）算法。尽管如此，作为迄今为止世界上最为广泛使用和流行的一种分组密码算法，DES 对于推动密码理论的发展和应用起了重大作用，对于掌握分组密码的基本理论设计思想和实际应用仍然有着重要的参考价值。

DES 加密算法如图 3-9 所示，它是一个 16-轮的迭代型密码，使用 56 比特的密钥来加密 64 比特的明文。其加、解密算法一样，但加、解密时所使用的子密钥的顺序刚好相反。下面是关于如何实现 DES 算法的语言性描述。

1．加密过程

（1）将一个 64 位明文分组 M 通过一个固定初始置换 IP 进行置换，获得 M_0。我们把这个过程记作 $M_0=IP（M）=L_0R_0$，这里 L_0 是 M_0 的前 32 比特，R_0 是 M_0 的后 32 比特。初始置换是将明文 M 中数据的排列顺序按一定的规则重新排列，而生成新的数据序列的过程。

它不会影响 DES 算法本身的安全性，其意义在于打乱输入分组 M 的 ASCII 码字划分关系。初始置换 IP 如表 3-1 所示，其含义是，将分组中原来各比特的位置上的数据用初始置换 IP 表中指示的相应位置的数据替换，即原第 1 位用原 58 位替换，第 2 位用原第 50 位替换，……，原第 64 位用原第 7 位替换。

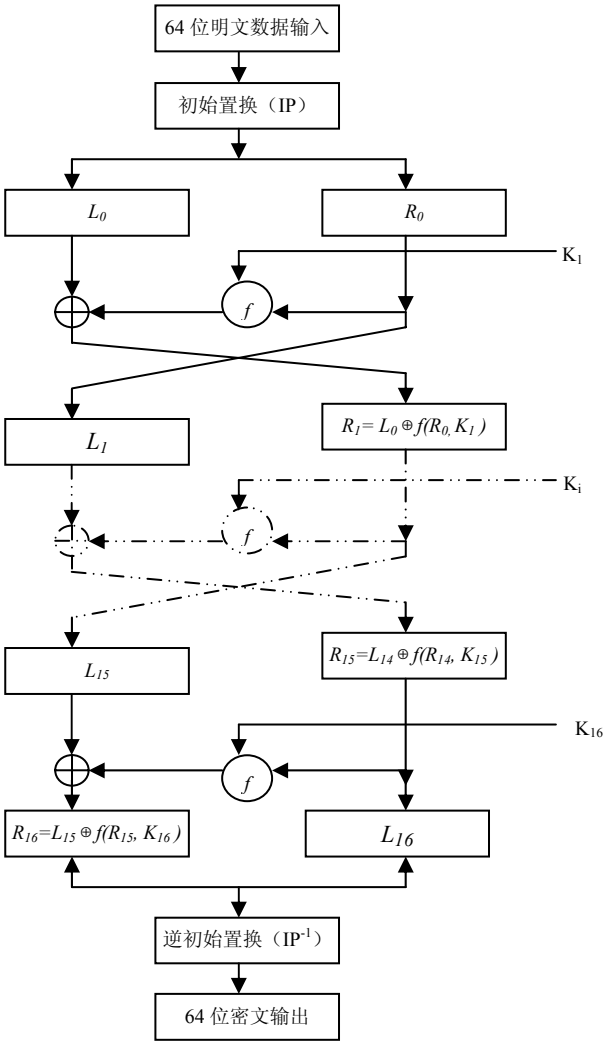


图 3-9　DES 加密算法图示

表 3-1　初始置换 IP

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

（2）在进行初始置换后，按照以下规则计算 L_i 和 R_i：

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

上述规则中，K_i（$1 \le i \le 16$）是密钥 K 的函数，长度均为 48 比特，我们称其为子密钥，关于 K_i 的生成将在下面描述。f 是一个函数，其计算过程也将在下面描述。

（3）对比特串 $R_{16}L_{16}$ 应用初始置换 IP 的逆置换 IP^{-1}，获得密文 C，即 $C = IP^{-1}(R_{16}L_{16})$。注意最后一次迭代后，左边和右边未交换，而将 $R_{16}L_{16}$ 作为 IP^{-1} 的输入，目的是为了使算法可同时用于加密与解密。其中初始置换 IP 的逆置换 IP^{-1} 如表 3-2 所示。当然，读者也完全可以自己写出这个逆置换。

表 3-2　初始置换 IP 的逆置换 IP^{-1}

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31

38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

2．解密过程

解密采用同一算法实现，把密文 C 作为输入，且倒过来使用密钥方案即以逆序 K_{16}，K_{15}，…，K_1 密钥方案，输出明文 M。

3．子密钥的生成

DES 描述文档中给出的密钥长度是 64 比特，从左到右，其第 8、16、……、64 位为奇偶校验位，因此实际上使用的密钥长度为 56 比特。

如前所述，DES 算法由 16 轮运算构成，每轮运算使用的子密钥各不相同，每个子密钥的长度为 48 比特，而 DES 使用的密钥是 56 比特，那么如何生成 16 个密钥呢？实际上，这 16 个密钥都是分别从 56 比特密钥中挑选出来的 48 比特数据构成的。挑选的过程如下所述：

（1）对这 56 比特密钥做一个置换，置换表如表 3-3 所示。

表 3-3　密钥置换表

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	50	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

这个置换表的含义是，输出的最左边比特是密钥的第 57 位，第 2 比特是密钥的第 49 位，依次类推。在这个表中，第 8、16、……、64 位没有出现，从中也可以看出实际使用的密钥长度是 56 比特。

（2）将这 56 比特分为两部分，每部分为 28 比特，第一部分由前面 28 比特构成，记为 C_0；第二部分由后面 28 比特构成，记为 D_0。然后根据轮数，这两部分分别左移 1 到 2 位。具体是，在轮数 i = 1、2、9、16 时，移动一个位置，当 i = 3、4、5、6、7、8、10、11、12、13、14、15 时，移动两个位置。应当注意，每轮移位是在上一轮移位的基础上进行的。也就是说，C_1 是 C_0 循环左移 1 位而成，C_2 是 C_1 循环左移 1 位构成，依次类推。同样，D_1 是 D_0 循环左移 1 位而成，D_2 是 D_1 循环左移 1 位而成，依次类推。

（3）每次需要子密钥 K_i 时，需要从 C_i 和 D_i 的 56 比特挑选出 48 比特，如表 3-4 所示。

表 3-4　挑选生成 48 比特 K_i

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

表 3-4 的含义是，如表中第 n 个数值为 m，则表示输出的子密钥 K_i 的第 n 比特为（C_iD_i）的第 m 比特。

经过上述几步运算，就得到了全部 16 个 48 比特的子密钥 K_i（1≤i≤16）。

4．f 函数

回忆一下前述的 DES 加解密过程，在该过程中需要一个 f 函数。该函数对数据的一半与密钥做运算，并将生成的结果异或到另一半中。下面将描述 f 函数。

注意到 f 函数处理的数据是 32 比特的数据（L 或 R）和 48 比特的密钥（K_i）。因此在运算时，f 函数需要将 32 比特的数据扩展为 48 比特的数据并与 48 比特的数据异或，随后还需要将异或得到的结果压缩回 32 比特。f 函数的构成如图 3-10 所示。

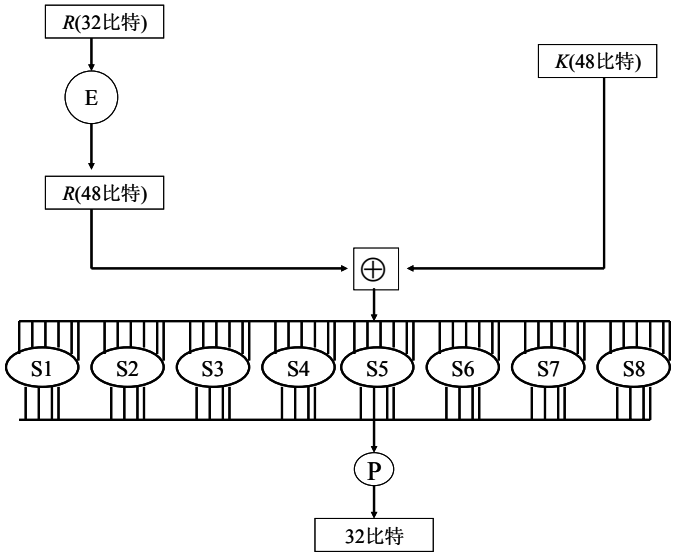


图 3-10　f函数的构成

具体步骤如下：

（1）利用一个固定扩展 E 将 R_i 扩展一个长度为 48 的比特串 $E(R_i)$，扩展 E 如表 3-5 所示。

表 3-5　扩展 E

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

表 3-5 的置换称为扩展置换，其方法是，将原始 32 比特数据分为 8 组，每 1 组 4 比特数据加上其左右两边的数据后扩展为 6 比特数据（将第 1 比特左边视为第 32 特），即 32 比特数据扩展为 48 比特。具体而言，就是原始数据的第 1、2、3、4 比特扩展成原始数据的第 32、1、2、3、4、5 比特，原始数据的第 5、6、7、8 比特扩展成原始数据的第 4、5、6、7、8、9 比特，依次类推，原始数据的 29、30、31、32 比特扩展成原始数据的第 28、29、30、31、32、1 比特。

（2）计算 $E（R_i）\oplus K_{i+1}$,并将结果分成 8 个长度为 6 的比特串，记为：

$$E（R_i）\oplus K_{i+1} = T_1T_2T_3T_4T_5T_6T_7\ T_8。$$

（3）将数据压缩回 32 比特。这个过程通过“S 盒替代”实现。所谓 S 盒是一组变换，这些变换输入 6 比特，输出 4 比特，共有 8 个 S 盒 S_1、S_2、S_3、S_4、S_5、S_6、S_7、S_8。每一个 S_i 是一个固定的 4×16 阶矩阵，他们的元素来自于 0~15 这 16 个整数，如表 3-6 所示。

表 3-6　S 盒

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	

4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

使用这些 S 盒的方法是将 T_i 视作 6 比特的数值，查询 S_i 表得到该表的第 T_i 项就是输出的数值。注意，由于 T_i 的取值范围从 0 到 63（即其二进制数值最大为 111111），所以该表中数值的编号是从 0 开始的。也就是说，查询 S 盒时应该说第 0 个数值、第 1 个数值……，直至第 63 个数值。例如 T_2 = 101100，即等价于十进制的 44，查询 S_2 表的第 44 个数值为 9，也就是输出的 4 位二进制数为 1001。

（4）P 置换。将长度为 32 比特的第（3）步输出结果通过一个固定的置换 P 得到最终的 32 比特。P 置换如表 3-7 所示。

表 3-7　P 置换

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

5．DES 算法的安全性

在 DES 算法中，有一个“弱密钥”的概念。这里我们将 DES 加密运算记为 DES（*K,X*）（*X* 表示任意 64 位的比特串，*K* 为密钥），DES 解密运算记为 DES^{-1}（*K,X*）。如存在一个 *K*，使得 DES（*K,X*）= DES^{-1}（*K,X*），则 *K* 为弱密钥；如存在两个密钥 *K* 和 *K'*，使得 DES（*K,X*）= DES^{-1}（*K',X*），则 *K* 为半弱密钥（当然 *K'*也是）。使用这些密钥，在选择明文攻击下，会使 DES 加密变得很脆弱。在 DES 算法中有至少有 4 个弱密钥和 12 个半弱密钥，但目前还没有证明除这些弱密钥和半弱密钥外，还有其它的弱密钥和半弱密钥外。由于 DES 是采用 56 比特的加密算法，所以总共有 2^{56} 种可能的密钥组合，选择到一个弱密钥的可能性是很小的。不会危及到 DES 的安全性。

对 DES 最中肯的批评是，密钥空间的规模 2^{56} 对实际安全而言确实太小了。早在 20 世纪 70 年代，就有人提出建造一台特殊目的的机器来实施已知明文攻击，实质就是用穷举法破译 DES 密码。1997 年 1 月 28 日，美国的 RSA 数据安全公司在 RSA 安全年会上公布了一项“秘密密钥挑战”竞赛，悬赏一万美金破译密钥长度为 56 比特的 DES 算法。美国克罗拉多州的程序员 Verser 从 1997 年 3 月 13 日起，用了 96 天的时间，在 Internet 上数万名志愿者的协同工作下，于 6 月 17 日成功地找到了 DES 的密钥，获得了 RSA 公司颁发的一万美金的奖励。1998 年 7 月 22 日信息，电子前沿基金会（Electronic Frontier Foundtion）花费 25 万美金制造了一台电脑，在 56 小时内破译了 56 位的 DES。

迄今为止，S 盒的设计原理尚未完全公开，一些密码学家怀疑 S 盒里隐藏了“陷门”，使知道这个秘密的人可以很容易地进行密文解密。不过到目前为止，还没有证据能证明 DES 里确实存在陷门。

6．三重 DES

三重 DES 是在 DES 基础上发展起来的加密算法，已成为商用标准，在密钥管理标准 ANS X.917 和 ISO 8732 中被采用。其核心是为了解决 DES 密钥过短的问题，使用两个密钥执行三次 DES 算法。加密方式是在两个密钥的控制下，实施加密—解密—加密的过程，整个过程如图 3-11 所示。

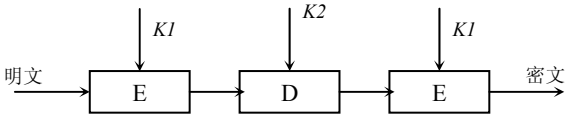


图 3-11　三重 DES 加密过程

解密过程如图 3-12

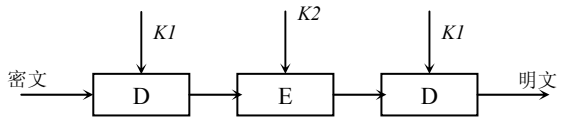


图 3-12　三重 DES 解密过程

之所以在加密、解密过程中使用两个而不使用三个密钥，是因为两个个密钥合起来长度以有 112 比特，这对商用已足够了，如使用总长为 168 比特的三个密钥，则会产生不必要的开销。

为什么在加密时采用 E-D-E，而不是 E-E-E 呢？这是为了与现有的 DES 系统向后兼容性。其实不论是加密还是解密过程，都是在两个 64 比特的数之间的一种映射。从密码的角度来看，这种映射的作用是一样的。但是，使用 E-D-E 的好处是当 *K1=K2* 时，三重 DES 就和 DES 一样，这样有利于推广使用三重 DES。

3.3.3　其它分组密码算法

1．IDEA 算法

IDEA（国际数据加密算法，International Data Encryption Algorithm）是 Xuejia Lai（来学嘉）、James Massey 等人提出的加密算法。早在 1990 年，Xuejia　Lai 等人在 EuroCrypt'90 年会上提出了分组密码建议 PES（Proposed Encryption Standard）。在 EuroCrypt'91 年会上，Xuejia　Lai 等人又提出了 PES 的修正版 IPES（Improved PES）。目前 IPES 已经商品化，并改名为 IDEA。

IDEA 是一个分组长度为 64 比特的分组密码算法，密钥长度为 128 比特，同一个算法既能用于加密又能用于解密。该算法的设计原则是一种“来自于不同代数群的混合运算”。三个代数群进行混合运算，无论用硬件还是软件，它们都易于实现。该算法涉及到三种运算：异或、模 2^{16} 加、模 $2^{16}+1$ 乘，三种运算都在 16 比特子分组上进行。

类似于 DES，IDEA 算法也是一种分组加密算法，它设计了一系列加密轮次，每轮加密都使用从完整的加密密钥中生成的一个子密钥。与 DES 的不同处在于，它采用软件实现和采用硬件实现同样快速。

IDEA 算法使用了 52 个子密钥（8 轮中的每一轮需要 6 个，其它 4 个用于输出变换）。首先，将 128 比特密钥分成 8 个 16 比特子密钥。这些是算法的第一批 8 个子密钥（第一轮 6 个，第二轮的头 2 个）。然后，密钥向左环移动 25 位产生另外 8 个子密钥，如此进行直到算法结束。

IDEA 算法的加密过程是，将 64 比特数据分组分成 4 个 16 比特子分组：*X1*、*X2*、*X3* 和 *X4*。这四个子分组成为算法的第一轮输入。在每一轮中，四个子分组相互间相异或，相加，相乘，且与 6 个 16 比特子密钥相异或，相加，相乘。在轮与轮之间，第二和第三个子分组交换。最后在输出变换中四个子分组与四个子密钥进行运算。

在每一轮中，执行的顺序如下：

（1）*X1* 和第一个子密钥相乘　　（2）*X2* 和第二个子密钥相加

（3）*X3* 和第三个子密钥相加　　（4）*X4* 和第四个子密钥相乘

（5）将第 1 步和第 3 步的结果相异或　　（6）将第 2 步和第 4 步的结果相异或

（7）将第 5 步的结果与第五个子密钥相乘　　（8）将第 6 步和第 7 步的结果相加

（9）将第 8 步的结果与第六个子密钥相乘　　（10）将第 7 步和第 9 步的结果相加

（11）将第 1 步和第 9 步的结果相异或　　（12）将第 3 步和第 9 步的结果相异或

（13）将第 2 步和第 10 步的结果相异或　　（14）将第 4 步和第 10 步的结果相异或

每一轮的输出是第 11、12、13 和 14 步的结果形成的 4 个子分组。将中间两个分组交换（最后一轮除外）后，即为下一轮的输入。

经过 8 轮运算之后，有一个最终的输出变换：

（1）*X1* 和第一个子密钥相乘　　（2）*X2* 和第二个子密钥相加

（3）*X3* 和第三个子密钥相加　　（4）*X4* 和第四个子密钥相乘

最后，将这四步运算的结果连到一起就是所要产生的密文。

IDEA 的解密过程与加密过程基本上一样，只是解密密钥在从加密子密钥中导出时需要用到其它数学基础，这里就不再赘述，感兴趣的读者可以参考有关资料。

IDEA 的密钥长度是 128 比特，比 DES 长两倍多，假定穷举法攻击有效的话，那么为获取密钥需要 2^{128} 次加密运算，即使设计一种每秒可以试验 10 亿个密钥的专用芯片，并将 10 亿片这样的芯片来并行处理，仍需 10^{13} 年才能解决问题。另外，设计者已尽力使这个算法抗差分密码分析的攻击，Xuejia Lai 已证明 IDEA 算法在其 8 轮迭代的第 4 轮之后便不受差分密码分析的影响了。目前，密码学界尚未发现 IDEA 算法存在明显的缺陷。但是，之所以 IDEA 算法没有取代 DES 算法，一方面是因为 IDEA 算法存在专利问题，另一方面是人们一直在对 IDEA 算法进行深入分析以研究其是否存在安全问题。

2．AES 算法

1997 年 9 月，美国 NIST 公开征集 AES 方案，以替代 DES。NIST 征集算法的前提条件是算法的设计原理必须公开，而且要求算法必须是免费的，也就是说对算法的使用不应该有任何专利限制。经评审，1999 年 8 月，以下 5 个方案成为最终候选方案：MARS、RC6、Rijndael、Serpent 和 Twofish。2000 年 10 月，由比利时的 Joan Daemen 和 Vincent Rijmen 提出的 Rijndael 算法最终胜出，成为 AES 标准。

Rijndael 算法的分组大小和密钥长度可以有多种选择，这两个参数可以单独从 128、160、192、224 和 256 比特中任意选取（密钥长度和分组长度可以不一样）。AES 算法 Rijndael 算法标准化后规定分组大小为 128 比特，密钥长度可以是 128、192 或 256 比特，并将其称为 AES-128、AES-192 和 AES-256。

Rijndael 算法基于非常巧妙的数学原理，即基于域上点的运算设计的算法，通过特别的设计使得加密和解密过程基本一致（加密和解密的轮运算可以使用相同的运算结构），有关的设计理论比较复杂，感兴趣的读者可以到 NIST 官方网站查看该算法的详细说明以及密码学界对其所作的分析。

3.4　公钥密码

前面几节讨论的密码体制主要是单钥密码体制，单钥密码体制的一个严重的缺点就是在任何密文传输之前，通信双方必须使用一个安全渠道协商加密密钥。在实际中，做到这一点是很难的。还有，如何为数字化的信息或文件提供一种类似于为书面文件手写签字的方法，这也是单钥密码体制难于解决的问题。1976 年，W.Diffie 和 M.E.Hellman 发表了《密码学中的新方向》（*New Directions in Cryptography*）一文，提出了公钥密码体制的观点，使密码学发生了一场变革。1977 年由 Rivest、Shamir 和 Adleman 提出了第一个比较完善的公钥密码体制 RSA。公开密码体制很好地解答了上面两个问题。

在公钥密码中，最著名也是应用最广的密码算法是 RSA 密码算法和椭圆曲线密码算法。

3.4.1　概述

在公钥密码体制中，公钥密码算法采用了两个相关密钥，将加密与解密能力分开。其中一个密钥是公开的，称为公钥，用于加密，另一个是用户专有的，因而是保密的，称为私钥，用于解密。公钥密码体制具有如下重要特性：已知密码算法和公钥，求解私钥，计算上是不可行的。公钥密码算法按下述步骤对信息实施保护，为了叙述方便，我们把信息发送方设为

A，信息接收方为 B：

（1）要求信息接收方 B，产生一对密钥 PK_B 和 SK_B，其中是 PK_B 为公钥，SK_B 为私钥。

（2）接收方 B 将 PK_B 公开，保密 SK_B。

（3）A 要想向 B 发送信息 M，则使用 B 的公钥 PK_B 加密 M，表示为 $C=E_{PK_B}(M)$。

（4）B 收到密文 C 后，则用自己的私钥 SK_B 解密，表示为 $M=D_{SK_B}(C)$。

公钥密码算法应满足如下要求：

（1）接收方 B 产生自己的公、私密钥对，在计算上是容易的。

（2）发送方 A 用接收方 B 的公钥对信息 M 加密以产生密文 C，在计算上是容易的。

（3）接收方 B 用自己的私钥对 C 解密，在计算上是容易的。

（4）攻击者由 B 的公钥求 B 的私钥，在计算上是不可行的。

（5）攻击者由密文 C 和 B 的公钥，恢复明文在计算上是不可行的。

（6）加解密次序可以交换（但不是对所有的算法都作要求）。

以上要求的本质在于求一个单向陷门函数，单向陷门函数是指满足下列条件的函数 f：

（1）给定 x，计算 $y=f(x)$ 是容易的；

（2）给定 y，计算 x 使 $x=f^{1}(y)$ 是困难的。（所谓困难是指计算上相当复杂，耗时极大，已失去实际意义）

（3）存在 δ，已知 δ 时，对给定的任何 y，若相应的 x 存在，则计算 x 使 $x=f^{1}(y)$ 是容易的。

我们把仅满足 1、2 两条的函数称为单向函数；第 3 条称为陷门性，δ 称为陷门信息。当用陷门函数 f 作为加密函数时，可将 f 公开，这相当于公钥；f 函数的设计者将 δ 保密，δ 相当于私钥。由于加密函数 f 是公开的，任何人都可以将信息 x 加密成 $y=f(x)$，然后送给函数的设计者（当然可以通过不安全信道传送）；由于设计者拥有 δ，他自然可以解出 $x=f^{1}(y)$。另外单向陷门函数的第 2 条性质表明窃听者由截获的密文 $y=f(x)$ 推测 x 是不可行的。

公钥密码算法不仅能用于保护传递信息的保密性，而且还能对发送方发送的信息提供验证，如 B 用自己的私钥 SK_B 对 M 加密，将 C 发往 A，A 用 B 的公钥 PK_A 对 C 解密。因为从 M 得到 C 是经过 B 的私钥 SK_B 加密的，只有 B 才能做到。因此 C 可当作 B 对 M 的数字签名。另一方面，任何人只要不知道 B 的私钥 SK_B 就不能篡改 M，所以以上过程获得了对信息来源和信息完整性的认证。以上认证过程中，由于信息是由 B 的私钥加密的，所以信息不能被他人篡改，但却能被他人窃听，这是因为任何人都能用 B 的公钥对信息进行解密，为了提供认证功能和保密，可用双重加解密。B 首先用自己的私钥对信息 M 加密，再用 A 的公钥进行第二次加密。解密过程是 A 用自己的私钥，后用 B 的公钥对收到的密文进行两次解密。在本章的后面还会继续介绍公钥密码算法在签名方面的应用。

3.4.2 RSA 算法

RSA 公钥算法是由 Rivest、Shamir 和 Adleman 在 1978 年提出来的，并以他们的名字命名该算法。RSA 算法的数学基础是初等数论中因子分解理论和欧拉定理，并建立在大整数因子分解的困难性之上。

1．数学基础

1）同余

一个大于 1 的整数如果只能被 1 和它自身整除，而不能被其它正整数整除，那么这个整数称为素数（质数）。

用 gcd（a，b）表示整数 a 和 b 的最大公因子，那么当 gcd（a，b）= 1 时，则称为 a 和 b 互素。

如果整数 a 和 b 的差 a-b 能被另一个整数 r 整除，即 $r \mid a-b$，则称 a、b 关于模 r 同余，用符号 $a \equiv b \pmod r$ 表示。（即 a 和 b 有相同的余数）

同余关系是一个等价关系，即满足：

（1）自反性，即 $a \equiv a$（mod r）。

（2）对称性，若 $a \equiv b$（mod r），则 $b \equiv a$（mod r）。

（3）传递性，如果 $a \equiv b$（mod r），$b \equiv c$（mod r），则 $a \equiv c$（mod r）。

下面我们给出消去律定理：

消去律定理：如果 gcd（c，p）=1，即 c、p 互素，则由

$$ac \equiv bc \bmod p$$

可以推出，

$$a \equiv b \bmod p$$

该定理的证明只用到非常初等的数学知识，请读者自行证明。

此外，我们在这里定义取模运算，即对于正整数 a 和 b，$a \bmod b$ 表示 a 除以 b 的余数。模运算具有以下性质（同样，这些性质的证明只需要使用初等数学知识，这里不再证明）：

（1）[（$a \bmod n$）+（$b \bmod n$）]mod n =（a+b）mod n

（2）[（$a \bmod n$）−（$b \bmod n$）]mod n =（a−b）mod n

（3）[（$a \bmod n$）*（$b \bmod n$）]mod n =（a*b）mod n

2）欧拉函数和欧拉定理

欧拉函数 φ（n）是这样定义的：当 n = 1 时，φ（1）= 1；当 n＞1 时，φ（n）等于比 n 小而与 n 互素的正整数的个数。显然，对于素数 p，φ（p）= p-1。

下面我们证明，对于两个素数 p、q，它们的乘积 $n = pq$ 满足 φ（n）=（p-1）（q-1）。

证明：

对于 $n = pq$，小于 n 的集合为{1,2,3,…,（pq-1）}，不与 n 互素的集合有两个，分别是{p,2p,…,（q-1）p}和{q,2q,…,（p-1）q}，由于 p 和 q 是互素的，所以上面两个集合中没有共同的元素。于是，

φ（n）= pq -1-（q-1+ p-1）=（p-1）（q-1）= φ（p-1）φ（q-1）

证毕。

欧拉定理：若整数 a 与整数 n 互素，则 $a^{\varphi(n)} \equiv 1$（mod n）。

证明：

定义小于 n 且和 n 互素的正整数构成的集合为 Z^*_n，显然，Z^*_n 中的数目个数即$|Z^*_n| = \varphi$（n）。

令 $Z^*_n = \{x_1, x_2, ..., x_{\varphi(n)}\}$，考虑集合

$$S = \{ ax_1 \bmod n, ax_2 \bmod n, ..., ax_{\varphi(n)} \bmod n\}$$

由于 a、n 互素，x_i 也与 n 互素，则 ax_i 也一定于 n 互素。因此，对任意 x_i，$ax_i \bmod n$ 必然是 Z^*_n 的一个元素。

对于 Z^*_n 中两个不同的元素 x_i 和 x_j，如果 $x_i \neq x_j$，则

$$ax_i \bmod n \neq ax_j \bmod n$$

这是因为，如果 $ax_i \bmod n = ax_j \bmod n$，则根据消去律，$x_i \bmod n = x_j \bmod n$。由此推出 x_i 必须等于 x_j，这与 x_i 和 x_j 不同相矛盾。

所以很明显，$S = Z^*_n$。

那么，根据模运算的性质和 $S = Z^*_n$ 这一结论，可知

$$\begin{aligned}&（ax_1 * ax_2 * ... * ax_{\varphi(n)}）\bmod n\\ =\ &（ax_1 \bmod n * ax_2 \bmod n * \ ... * ax_{\varphi(n)} \bmod n）\bmod n\\ =\ &（x_1 * x_2 * ... * x_{\varphi(n)}）\bmod n\end{aligned}$$

考虑上面等式左边和右边，左边等于

$$[a^{\varphi(n)} *（x_1 * x_2 * ... * x_{\varphi(n)}）] \bmod n$$

右边是（$x_1 * x_2 * ... * x_{\varphi(n)}$）mod n

而（$x_1 * x_2 * ... * x_{\varphi(n)}$）和 n 互素，根据消去律，就得到：

$$a^{\varphi(n)} \equiv 1 \bmod n$$

证毕。

欧拉定理的推论是，对于互素的数 a 和 n，满足 $a^{\varphi(n)+1} \equiv a \bmod n$。这个推论对证明 RSA 算法非常关键。

2．算法描述

1）密钥对的产生

产生 RSA 密钥的过程如下所述：

（1）选择两个大素数 p 和 q。

（2）计算：$n = pq$，$\varphi(n) = (p-1)(q-1)$。

（3）随机选择一整数 e，要求 e 和 $\varphi(n)$ 互素。

（4）找到一个整数 d，满足

$$ed \equiv 1 (\bmod \varphi(n))$$

只要 e 和 n 满足以上条件，d 肯定是存在的。由于 e 和 $\varphi(n)$ 互素，用 e 乘以 $\varphi(n)$ 的完全余数集合中的每一个元素后再模 $\varphi(n)$，得到的余数将以不同的次数涵盖 $\varphi(n)$ 的完全余数集合中的所有数，则肯定有一个余数为 1。我们在前面证明欧拉定理时，已经证明过这一结论。

最后，e 和 n 便是 RSA 的公钥，d 是私钥。此时 p 和 q 不再需要，它们应该被舍弃掉，但绝不可泄漏。

2）加密、解密

对 m 作加密运算如下：

$$c = m^e (\bmod n)$$

得到的 c 即为密文，即密文 c 为 m 的 e 次方除以 n 的余数。

对密文的解密运算如下：

$$m = c^d (\bmod n)$$

解密运算的结果是得到原来的明文 m，即明文 m 为 c 的 d 次方除以 n 的余数。

3）算法证明

RSA 算法的证明过程如下：

因为 $ed \equiv 1 (\bmod \varphi(n))$，可将 ed 表示为：

$$ed = k*\varphi(n) + 1$$，其中 k 为任意整数。

将 c 用 $m^e (\bmod n)$ 替换后，计算 $c^d (\bmod n)$：

$$c^d (\bmod n) = (m^e)^d \bmod n = m^{ed} \bmod n = m^{k\varphi(n)+1} \bmod n$$

又由欧拉定理的推论 $m^{\varphi(n)+1} \equiv m (\bmod n)$，有：

$$m^{k\varphi(n)+1} \equiv m (\bmod n)$$

因此，

$$m^{k\varphi(n)+1} \bmod n = m \bmod n。$$

由于 m 小于 n，因此，

$$m \bmod n = m$$

即 $c^d (\bmod n) = m$，解密的结果是得到明文 m。

3．加解密过程举例

为了让读者进一步了解 RSA 的加解密过程，我们在下面举一个简单的例子说明这一过程。

取两个素数 $p = 7$，$q = 17$，计算出 $n = pq = 7 \times 17 = 119$，于是得到 $\varphi(n)$：

$$\varphi（n）=（p-1）（q-1）=96。$$

选择一个与 96 互素的正整数 e，我们选 $e=5$，然后求 d（实际应用中，这个 d 可以采用扩展欧几里德算法求出）：

$$5d=1 \bmod 96$$

解出 $d=77$，因为 $ed=5\times77=385=4\times96+1=1 \bmod 96$。

于是，公钥 $PK=（e,n）=（5,119）$，而密钥 $SK=77$。

现在对明文进行加密。设明文分组是 $m=19$。用公钥加密时，先计算 $m^e=19^5=2476099$。再除以 119，得出商为 20807，余数为 66。66 就是对应于明文 19 的密文 c 的值。

在用密钥 $SK=77$ 进行解密时，先计算 $c^d=66^{77}=1.27\ldots\times10^{140}$。再除以 119，得出商为 $1.06\ldots\times10^{138}$，余数为 19。此余数即解密后应得出的明文 c。

图 3-13 展示了这一过程。

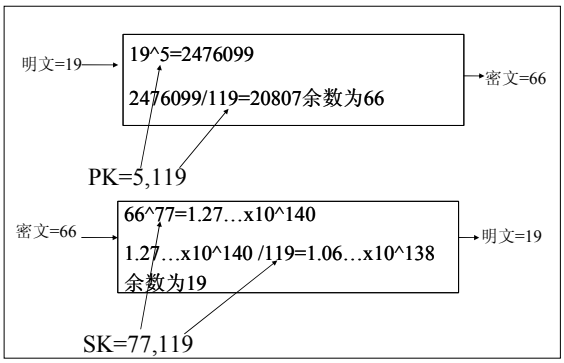


图 3-13　RSA 加解密过程举例

4．RSA 算法的安全性

RSA 的安全性是基于大整数因子分解问题的难解性，目前尽管尚未从理论上证明大整数的因子分解问题是难解问题，但迄今还没有找到一个有效算法的事实，使得大整数的因子分解问题成为众所周知的难题，这是 RSA 的基础。如果 RSA 的模数 n 被成功分解为 pq，则立即可算出 $\varphi（n）=（p-1）（q-1）$ 和 d，因此攻击成功。而且分解 n 也是攻击 RSA 最显然的方法。随着计算能力的不断提高和分解算法的进一步改善，原来认为不可能被分解的大数可以被成功分解，因此为了抵抗现有的整数分解算法，保证算法的安全性，对 p 和 q 的选取提出了以下要求：

（1）$|p-q|$很大，且通常 p 和 q 的长度相同；

（2）$p-1$ 和 $q-1$ 分别含有大素因子 p_1 和 q_1；

（3）p_1-1 和 q_1-1 分别含有大素因子 p_2 和 q_2；

（4）$p+1$ 和 $q+1$ 分别含有大素因子 p_3 和 q_3。

RSA 密钥对生成时要在两个大素数的寻找方面花时间，一般都是随机生成一个大奇数，然后用素性测试方法对得到的数进行测试，判断其是否为素数。由于受到素数产生技术的限制，RSA 难以做到一次一密，这也是其不足之一。

用于大因数分解的软件和硬件有很多，且耗费越来越小，速度越来越快，这为 RSA 算法的安全性造成了很大威胁。512 比特的 RSA 早已被证明是不安全的，而 1024 比特 RSA 的安全性在几年之前也有人提出了置疑。目前很多标准中都要求使用 2048 比特的 RSA。

为了提高加密速度，通常取 e 为特定的小整数，如 EDI（电子数据交换）国际标准中规定 $e=2^{16}+1$，ISO/IEC 9796 甚至允许取 $e=3$。这样导致加密速度一般比解密速度快 10 倍以上。尽管如此，与对称密码体制相比（如 DES），RSA 的加、解密速度还是太慢，所以它很少用于数据的加密，而一般用于数字签名、密钥管理和认证方面。

3.4.3 椭圆曲线密码算法

椭圆曲线密码（ECC，Elliptic curve cryptography）是基于椭圆曲线算数的一种公钥密码方法。椭圆曲线在密码学中的使用是在 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出的。椭圆曲线密码有一些突出的优点：密钥长度短，抗攻击性强，单位比特的安全性强度较高，例如 160 比特的 ECC 与 1024 比特的 RSA 有相同的安全强度；此外，ECC 的计算量小，处理速度快，例如在相同的强度下，用 160 比特的 ECC 进行加、解密或数字签名要比用 1024 比特的 RSA 块大约 10 倍。目前，ECC 算法已经成为一种非常流行的公钥密码算法。

由于学习椭圆曲线密码体制需要较多的数学知识，本小节仅介绍了一些基本概念，感兴趣的读者可以参考有关资料。

1．椭圆曲线

实数域上的椭圆曲线是指方程

$$y^2+axy+by=x^3+cx^2+dx+e$$

的所有解（x，y）$\in R\times R$（R 表示实数域），再加上一个无穷远点（我们记作 O）所构成的一个集合 E，其中 a，b，c，d，e 是满足某些简单条件的实数。

我们在 E 上定义加法运算，加法的运算规则如下：

对所有的 P，$Q\in E$

（1）O 是加法的单位元，有 $O=-O$。

（2）对椭圆曲线上的任何一点 P，有 $P+O=P=O+P$。

（3）如果 $P=(x_1, y_1)$，那么 $-P=(x_1, -y_1-ax_1-b)$

（4）如果 $Q=-P$，那么，$P+Q=O$

（5）如果 $P\neq O$，$Q\neq O$，$Q\neq -P$，$Q\neq P$，让 R 是过点 P 和 Q 的直线与 E 的交点，那么

$$Q+P=-R。$$

（6）Q 的倍数定义如下：在点 Q 作 E 的切线并找出另一交点 S，定义 $Q+Q=2Q=-S$。

结合（5），类似的可定义 $3Q=Q+Q+Q$，…，$nQ=Q+...+Q$。

我们可证明 E 关于上述定义的加法运算构成了一个交换群。

2．有限域上的椭圆曲线

实数是连续的，导致定义于其上的椭圆曲线也是连续的，但连续的椭圆曲线并不适用于加密，所以在密码学上我们关心的是定义在有限域上的椭圆曲线。

有限域 F 上的椭圆曲线是指方程

$$y^2+axy+by=x^3+cx^2+dx+e$$

的所有解（x，y）$\in F\times F$，再加上一个无穷远点（我们记作 O）所构成的一个集合 E，其中 a，b，c，d，$e\in F$，且满足某些简单的条件。

由上面有限域 F 上椭圆曲线的定义，可以看出有限域上的椭圆曲线是离散的。下面我们介绍定义于有限域 Z_p（$p>3$ 是素数）上的一类简单且常用的椭圆曲线 $y^2=x^3+ax+b$，至于其它类型有限域上的椭圆曲线，有兴趣的读者可参阅有关的文献。

有限域 Z_p（$p>3$ 是素数）上的椭圆曲线 $y^2=x^3+ax+b$ 是由一个称为无穷远点的 O 和满足同余方程

$$y^2\equiv x^3+ax+b\ (\mathrm{mod}\ p)$$

的解（x，y）$\in Z_p\times Z_p$ 组成的集合 E，其中，a、$b\in Z_p$，并满足

$$4a^3+27b^2\ (\mathrm{mod}\ p)\neq 0。$$

为了以后叙述方便，我们把 Z_p 上的这类椭圆曲线记为 E_p（a，b)。与实数域上的椭圆曲线上的加法定义方式相同，椭圆曲线 E_p（a，b)上的加法定义如下（所有的运算都在 Z_p 上）：对任意 $P=(x_1, y_1)$，$Q=(x_2, y_2)\in E$，

$$P+Q=\begin{cases} O & \text{如果 } x_1=x_2,\ y_1=-y_2 \\ (x_3,\ y_3) & \text{否则} \end{cases}$$

其中

$$x_3=\lambda^2-x_2-x_1$$
$$y_3=\lambda(x_1-x_3)\ -y_1$$

且

$$\lambda=\begin{cases} (y_2-y_1)(x_2-x_1)^{-1} & P\neq Q \\ (3x_1^2+a)(2y_1)^{-1} & P=Q \end{cases}$$

最后对所有的 $P\in E$，定义 $P+(-P)=O$。

注意，Z_p（$p>3$ 是素数）上的椭圆曲线没有实数域上的椭圆曲线的直观的几何解释。然而可以验证，E_p（a，b） 关于上述定义的加法运算仍然构成了一个交换群。

若 E 是有限域 Z_p 上的椭圆曲线，$P\in E$，则 P 的阶是满足

$$nP=P+P+...+P=O$$

的最小正整数 n，记为 ord（P），其中 O 是无穷远点。

若 E 是有限域 Z_p（$p>3$ 是素数）上的椭圆曲线，且 G 是 E 的一个循环子群，α 是 G 的生成元，$\beta\in G$。那么已知 α 和 β，求满足

$$n\alpha=\beta$$

的最小整数 n，称为椭圆曲线上的离散对数问题。

3．椭圆曲线上的密码

在这里我们只介绍椭圆曲线上的 Menezes－Vanstone 公钥密码体制，它是 EIGamal 公钥密码体制在椭圆曲线上的实现，1993 年由 A.J.Menezes 和 S.A.Vanstone 提出。

Menezes－Vanstone 公钥密码算法描述如下，为了叙述的方便，我们称发送方为 A，接收方为 B。

1）密钥的生成

（1）A 选一个大素数 p；

（2）A 选有限域 Z_p 上的一个椭圆曲线 E，且包含一个阶足够大的元素 α，α 的阶记为 $n=$ ord（α）；

（3）A 选取整数 d，满足 $1\le d\le n-1$，并计算 $\beta=d\alpha$；

（4）A 的公钥为（E，p，α，β，n），秘密密钥为 d。

2）加密

（1）B 获取 A 的公钥（E，p，α，β，n）；

（2）B 选取整数 k，满足 $1\le k\le n-1$，并计算 $y_0=k\alpha$ 和 $\delta=(c_1,\ c_2)=k\beta$；

（3）对明文 $x=(x_1,\ x_2)\in Z_p^*\times Z_p^*$ （$Z_p^*=Z_p-\{0\}$），B 计算

$$y_1=c_1x_1 \mod p$$
$$y_2=c_2x_2 \mod p$$

（4）B 得到密文 $y=(y_0,\ y_1,\ y_2)\in E\times Z_p^*\times Z_p^*$，并将它发送给 A。

3）解密

（1）A 收到 B 发给他的密文 $y=(y_0,\ y_1,\ y_2)$；

（2）A 计算 $d\,y_0=(c_1,\ c_2)$；

（3）A 分别计算 c_1 和 c_2 在 Z_p 上的逆元 c_1^{-1}，c_2^{-1}；

（4）A 获得明文

$$(c_1^{-1}y_1 \bmod p,\ c_2^{-1}y_2 \bmod p)=(c_1^{-1}c_1\,x_1 \bmod p,\ c_2^{-1}c_2x_2 \bmod p)=(x_1,\ x_2)=x。$$

4．ECC 的安全性

椭圆曲线密码的安全性，依赖于椭圆曲线离散对数问题（ECDLP）的难解性。从目前的研究结果来看，椭圆曲线离散对数问题（ECDLP）比有限域上的离散对数问题似乎更难以处理。迄今还没有出现类似于解有限域上的离散对数问题的 index-calculs 类型的亚指数时间的算法来解一般椭圆曲线离散对数问题（ECDLP）。这就意味着，可以在椭圆曲线密码体制中采用较小的数，以达到与使用更大的有限域同样的安全。

另外，如果定义于有限域 F 上的椭圆曲线 E 所含有的点的个数恰好等于有限域 F 含有的元素个数，这样的椭圆曲线我们称之为异常椭圆曲线，这类曲线易受攻击，在所有椭圆曲线密码体制中，该类曲线禁止使用。

3.5 散列函数

散列函数 h 是一公开函数，又称为杂凑函数、哈希（Hash）函数，用于将任意长的信息 M 映射为较短的、固定长度的一个值 h（M），称函数值 h（M）为消息 M 的消息摘要。消息摘要 h（M）是消息 M 中所有比特的函数，它提供了一种错误检测能力，即改变消息 M 中的任何一个比特或几个比特，h（M）都会发生变化。

散列函数在信息安全领域具有重要应用，它是实现数据完整性和身份认证的核心技术，本小节介绍了常用的 MD5（消息摘要算法 5，message-digest algorithm 5）和 SHA-1（安全散列算法 1，secure hash algorithm）。

3.5.1 概述

散列函数是一个从明文到密文的不可逆映射，只有加密过程，不能解密。散列函数的这种单向特性和输出数据的长度固定的特性使得它可以生成消息或其它数据块的“数字指纹”（也称为消息摘要、报文摘要）。这个“指纹”主要用于签名认证，签名认证同时还确保了消息或数据的完整性。根据散列函数的安全水平，我们将散列函数分为两类：即强无碰撞的散列函数和弱无碰撞的散列函数。

强无碰撞的散列函数是满足下列条件的一个散列函数 h：

（1）h 的输入可以是任意长度的任何消息或文件 M。

（2）h 的输出长度是固定的。

（3）给定 h 和 M，计算 h（M）是容易的。

（4）给定 h，和一个随机选择的 Z，寻找消息 M，使得 h（M）= Z，在计算上是不可行的。这一性质称为函数的单项性。

（5）给定 h，找两个不同的信息 $M1$ 和 $M2$，使得 h（$M1$）= h（$M2$），在计算上是不可行的。

弱无碰撞的散列函数是满足下列条件的一个散列函数 h：

（1）h 的输入可以是任意长度的任何消息或文件 M。

（2）h 的输出长度是固定的。

（3）给定 h 和 M，计算 h（M）是容易的。

（4）给定 h，和一个随机选择的 Z，寻找信息 M，使得 h（M）= Z，在计算上是不可行的。

（5）给定 h 和一个随机选择的信息 $M1$，要找另一个与 $M1$ 不同的信息 $M2$，使得 h（$M1$）= h（$M2$），在计算上是不可行的。

由强无碰撞的散列函数和弱无碰撞的散列函数的定义可知，强无碰撞的散列函数的安全性要比弱无碰撞的散列函数的要好。

3.5.2 MD5

MD5 在 90 年代初由 Mit Laboratory for Computer Science 和 Rsa Data Security Inc 的

Rivest 开发出来，经 MD2、MD3 和 MD4 发展而来。

MD5 以 512 比特分组来处理输入文本，每一分组又划分为 16 个 32 比特子分组。算法的输出由 4 个 32 比特分组组成，将它们级联形成一个 128 比特散列值。

1．算法描述

1）对消息 *M* 填充

填充消息 *M*，使其长度恰好为一个比 512 的倍数仅小 64 比特的数。填充方法是附一个 1 在消息后面，后接所要求的多个 0。

2）添加消息长度

在 1）的结果之后，用一个 64 比特的整数表示消息的原始长度（填充字节前消息 *M* 的长度），如果长度超过 64 比特所能表示的数据长度的范围，只保留长度范围的最后 64 比特，使添加后消息长度恰好是 512 比特的整数倍。这样我们可将消息 *M* 分为长为 512 比特的一系列分组 P_0、P_1、…、P_{L-1}。

这样，由于 MD5 的输入中包含原始消息的长度，攻击者必须找出具有相同散列值且长度相等的两条消息，或者找出两条长度不等但加入消息后散列值相同的报文，从而增加了攻击的难度。目前绝大多数散列函数均采用这种结构。

3）为四个寄存器 AA、BB、CC、DD 赋初始值

MD5 算法使用 128 比特长的缓冲区以存储中间结果和最终散列值，这个缓冲区可表示为四个寄存器 AA、BB、CC 和 DD，四个寄存器级联后构成了寄存器的当前值（记为 *CV*，这是散列计算的中间结果或最终的散列值）或初始值（记为 *IV*）。寄存器的初始化使用的是十六进制表示的数字：

AA = 01234567

BB = 89abcdef

CC = fedcba98

DD = 76543210

4）进行算法的主循环，主循环的次数是消息中 512 比特消息分组的数目 *L*

如图 3-14 所示，MD5 算法以每个 512 比特的分组 P_i（i = 0,1,…,L-1）和缓冲区 AA、BB、CC、DD 中的当前值 *CV*（即上一分组的计算结果）或初始值 *IV* 作为输入。总共需要计算 *L* 个主循环。

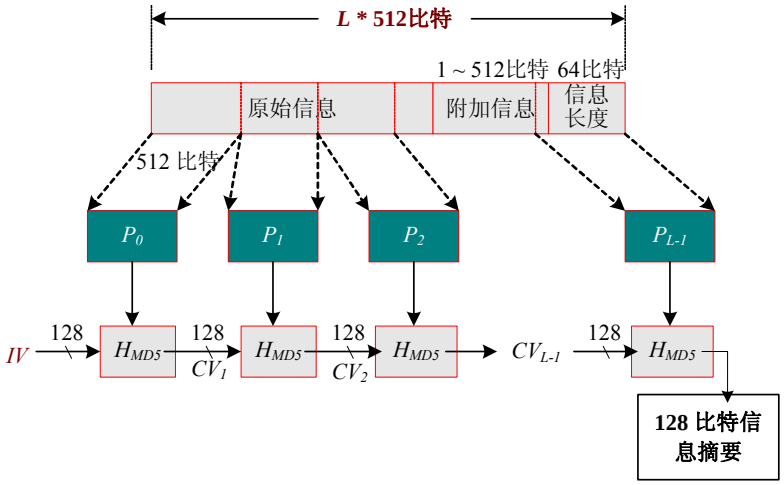


图 3-14　MD5 运行原理

每次主循环由四轮组成，四轮很相似。每一轮都进行 16 次操作（这样每一主循环进行 16×4=64 次操作）。在每一主循环的 64 次操作中，每次操作都要进行一次非线性函数计算，并且在这 64 次操作中共涉及到如下四个非线性函数：

$F(X,Y,Z) = (X\&Y) \mid ((\sim X)\ \&Z)$

$G(X,Y,Z) = (X\&Z) \mid (Y\&(\sim Z))$

$H(X,Y,Z) = X\hat{}Y\hat{}Z$

$I(X,Y,Z) = Y\hat{}(X\mid(\sim Z))$

其中，&表是与，|表是或，~表是非，^表是异或。为了以后叙述方便我们引入了如下标记：

$FF(a,b,c,d,p,s,t)$ 表示 $a = b+((a+(F(b,c,d)+p+t)<<<s)$

$GG(a,b,c,d,p,s,t)$ 表示 $a = b+((a+(G(b,c,d)+p+t)<<<s)$

$HH(a,b,c,d,p,s,t)$ 表示 $a = b+((a+(H(b,c,d)+p+t)<<<s)$

$II(a,b,c,d,p,s,t)$ 表示 $a = b+((a+(I(b,c,d)+p+t)<<<s)$

这里 a、b、c、d、p、t 都是 32 比特，$<<<s$ 表示循环左移 s 位。下面我们来描述一个主循环：

它的运行过程如下：

（1）将缓冲区 AA、BB、CC、DD 中的当前值复制到另外四个寄存器 A、B、C、D 中，AA 到 A，BB 到 B，CC 到 C，DD 到 D。并且将 512 比特分组 P_i 以每 32 比特为单位，划分为 16 个等长的子分组 M_j（$j = 0,1,\ldots,15$）。

（2）进行第一轮操作，使用 *FF* 函数，执行 16 次，使寄存器 A、B、C、D 的值发生变化（后面详细解释了 4 个寄存器的值的变化规律）

$FF(A,B,C,D,M_0,7,t_1)$　　$FF(D,A,B,C,M_1,12,t_2)$

$FF(C,D,A,B,M_2,17,t_3)$　　$FF(B,C,D,A,M_3,22,t_4)$

$FF(A,B,C,D,M_4,7,t_5)$　　$FF(D,A,B,C,M_5,12,t_6)$

$FF(C,D,A,B,M_6,17,t_7)$　　$FF(B,C,D,A,M_7,22,t_8)$

$FF(A,B,C,D,M_8,7,t_9)$　　$FF(D,A,B,C,M_9,12,t_{10})$

$FF(C,D,A,B,M_{10},17,t_{11})$　　$FF(B,C,D,A,M_{11},22,t_{12})$

$FF(A,B,C,D,M_{12},7,t_{13})$　　$FF(D,A,B,C,M_{13},12,t_{14})$

$FF(C,D,A,B,M_{14},17,t_{15})$　　$FF(B,C,D,A,M_{15},22,t_{16})$

（3）进行第二轮操作，使用 *GG* 函数，执行 16 次，使寄存器 A、B、C、D 的值发生变化

$GG(A,B,C,D,M_1,5,t_{17})$　　$GG(D,A,B,C,M_6,9,t_{18})$

$GG(C,D,A,B,M_{11},14,t_{19})$　　$GG(B,C,D,A,M_0,20,t_{20})$

$GG(A,B,C,D,M_5,5,t_{21})$　　$GG(D,A,B,C,M_{10},9,t_{22})$

$GG(C,D,A,B,M_{15},14,t_{23})$　　$GG(B,C,D,A,M_4,20,t_{24})$

$GG(A,B,C,D,M_9,5,t_{25})$　　$GG(D,A,B,C,M_{14},9,t_{26})$

$GG(C,D,A,B,M_3,14,t_{27})$　　$GG(B,C,D,A,M_8,20,t_{28})$

$GG(A,B,C,D,M_{13},5,t_{29})$　　$GG(D,A,B,C,M_2,9,t_{30})$

$GG(C,D,A,B,M_7,14,t_{31})$　　$GG(B,C,D,A,M_{12},20,t_{32})$

（4）进行第三轮操作，使用 *HH* 函数，执行 16 次，使寄存器 A、B、C、D 的值发生变化

$HH(A,B,C,D,M_5,4,t_{33})$　　$HH(D,A,B,C,M_8,11,t_{34})$

$HH(C,D,A,B,M_{11},16,t_{35})$　　$HH(B,C,D,A,M_{14},23,t_{36})$

$HH(A,B,C,D,M_1,4,t_{37})$　　$HH(D,A,B,C,M_4,11,t_{38})$

$HH(C,D,A,B,M_7,16,t_{39})$　　$HH(B,C,D,A,M_{10},23,t_{40})$

$HH(A,B,C,D,M_{13},4,t_{41})$　　$HH(D,A,B,C,M_0,11,t_{42})$

$HH(C,D,A,B,M_3,16,t_{43})$　　$HH(B,C,D,A,M_6,23,t_{44})$

HH（$A,B,C,D,M_9,4,t_{45}$）　　HH（$D,A,B,C,M_{12},11,t_{46}$）

HH（$C,D,A,B,M_{15},16,t_{47}$）　　HH（$B,C,D,A,M_2,23,t_{48}$）

（5）进行第四轮操作，使用 II 函数，执行 16 次，使寄存器 A、B、C、D 的值发生变化

II（$A,B,C,D,M_0,6,t_{49}$）　　II（$D,A,B,C,M_7,10,t_{50}$）

II（$C,D,A,B,M_{14},15,t_{51}$）　　II（$B,C,D,A,M_5,21,t_{52}$）

II（$A,B,C,D,M_{12},6,t_{53}$）　　II（$D,A,B,C,M_3,10,t_{54}$）

II（$C,D,A,B,M_{10},15,t_{55}$）　　II（$B,C,D,A,M_1,21,t_{56}$）

II（$A,B,C,D,M_8,6,t_{57}$）　　II（$D,A,B,C,M_{15},10,t_{58}$）

II（$C,D,A,B,M_6,15,t_{59}$）　　II（$B,C,D,A,M_{13},21,t_{60}$）

II（$A,B,C,D,M_4,6,t_{61}$）　　II（$D,A,B,C,M_{11},10,t_{62}$）

II（$C,D,A,B,M_2,15,t_{63}$）　　II（$B,C,D,A,M_9,21,t_{64}$）

在这 4 轮 64 次操作中，常数 t_i（i = 1,2, …,64），是 $2^{32}\times abs(sin(i))$的整数部分的十六进制表示，i 的单位是弧度。表 3-8 给出了各个 t_i 的值。

表 3-8　MD5 算法中 t_i 值

t_1=D76AA478	t_{17}=F61E2562	t_{33}=FFFA3942	t_{49}=F4292244
t_2=E8C7B756	t_{18}=C040B340	t_{34}=8771F681	t_{50}=432AFF97
t_3=242070DB	t_{19}=265E5A51	t_{35}=699D6122	t_{51}=AB9423A7
t_4=C1BDCEEE	t_{20}=E9B6C7AA	t_{36}=FDE5380C	t_{52}=FC93A039
t_5=F57COFAF	t_{21}=D62F105D	t_{37}=A4BEEA44	t_{53}=655B59C3
t_6=4787C62A	t_{22}=02441453	t_{38}=4BDECFA9	t_{54}=8F0CCC92
t_7=A8304613	t_{23}=D8A1E681	t_{39}=F6BB4B60	t_{55}=FFEFF47D
t_8=FD469501	t_{24}=E7D3FBC8	t_{40}=BEBFBC70	t_{56}=85845DD1
t_9=698098D8	t_{25}=21E1CDE6	t_{41}=289B7EC6	t_{57}=6FA87E4F
t_{10}=8B44F7AF	t_{26}=C33707D6	t_{42}=EAA127FA	t_{58}=FE2CE6E0
t_{11}=FFFF5BB1	t_{27}=F4D50D87	t_{43}=D4EF3085	t_{59}=A3014314
t_{12}=895CD7BE	t_{28}=455A14ED	t_{44}=04881D05	t_{60}=4E0811A1
t_{13}=6B901122	t_{29}=A9E3E905	t_{45}=D9D4D039	t_{61}=F7537E82
t_{14}=FD987193	t_{30}=FCEFA3F8	t_{46}=E6DB99E5	t_{62}=BD3AF235
t_{15}=A679438E	t_{31}=676F02D9	t_{47}=1F2A7CF8	t_{63}=2AD7D2BB
t_{16}=49B40821	t_{32}=8D2A4C8A	t_{48}=C4AC5665	t_{64}=EB86D391

（6）将 AA、BB、CC、DD 分别加上 A、B、C、D，然后用于下一分组数据继续运行算法。

图 3-15 表示了上述的 4 轮操作过程。

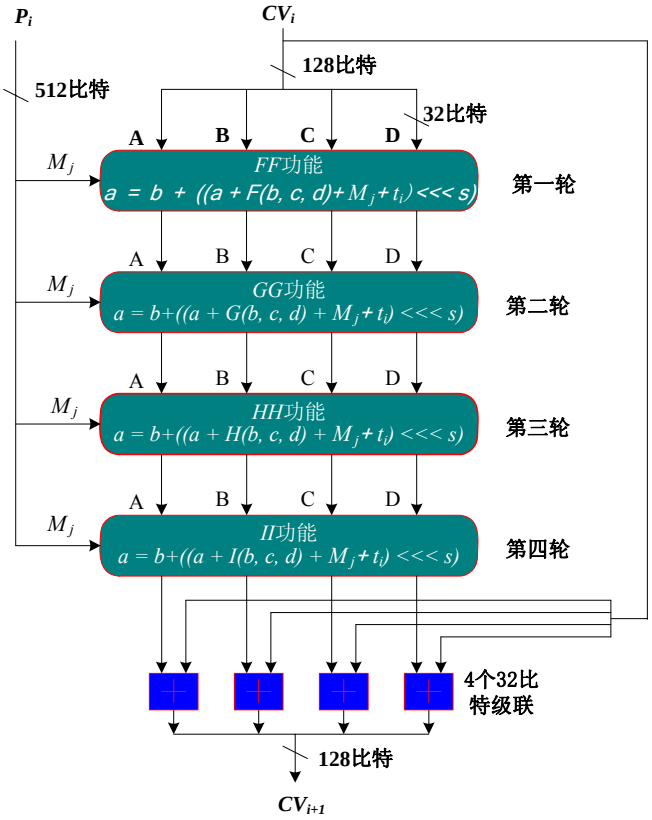


图 3-15　MD5 的 4 轮操作过程

在上述 4 轮操作过程中，还有三个细节问题需要解释。

一是在每一轮操作中执行每次运算后，寄存器 A、B、C、D 中的值需要交换，如图 3-16 所示。

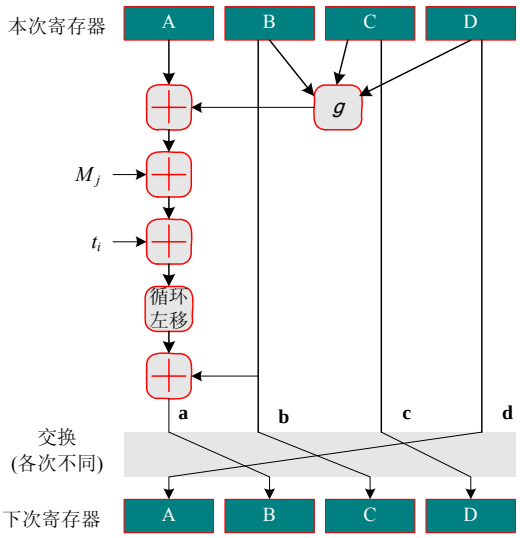


图 3-16　MD5 中寄存器值的变化

图 3-16 中的“g”表示 4 个非线性函数 F、G、H 或 I。以第 1 轮操作中的前两次运算为例，第 1 次执行 FF（$A,B,C,D,M_0,7,t_1$），第 2 次则执行 FF（$D,A,B,C,M_1,12,t_2$），即寄存器 D 的值赋给 A，寄存器 A 的值（这个值是执行 FF 运算的结果）赋给 B，寄存器 B 的值赋给 C，寄存器 C 的值赋给 D。在执行完第 2 次 FF 运算后，继续按照上面的规律交换寄存器值。

第二个需要解释的是 16 个 32 比特子分组的使用次序问题。在 4 轮操作中，每一个 32

比特的子分组只精确地使用 1 次。对第 1 轮来说，16 个子分组依次使用；而在第 2 轮，每一次使用的子分组序号依次为（1+5j）mod 16 的结果（j = 0,1,…,15），即分别为 M_1、M_6、…、M_{12}；在第 3 轮，每一次使用的子分组序号依次为（5+3j）mod 16 的结果（j = 0,1,…,15），即分别为 M_5、M_8、…、M_2；在第 4 轮，每一次使用的子分组序号依次为 7j mod 16 的结果（j = 0,1,…,15），即分别为 M_0、M_7、…、M_9。

第三个需要解释的是每一次运算中的循环左移量。每次的位移量都是不用的，我们在前面介绍 4 轮操作时已经给出了每一次的具体位移量，这些位移量集中如表 3-9 所示。

表 3-9　MD5 中各轮次的位移量

轮次	阶段															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	7	12	17	22	7	12	17	22	7	12	17	22	7	12	17	22
2	5	9	14	20	5	9	14	20	5	9	14	20	5	9	14	20
3	4	8	16	23	4	8	16	23	4	8	16	23	4	8	16	23
4	6	10	15	21	6	10	15	21	6	10	15	21	6	10	15	21

5）得出最后的 MD5 输出

最后的输出是 AA、BB、CC 和 DD 的级联。

2．MD5 的安全性

MD5 最后输出的散列值的每一比特都是所有输入比特的函数，因此获得了很好的混淆效果。但由于 MD5 较老，散列长度为 128 比特，随着计算机运算能力提高，找到“碰撞”是可能的。因此，在安全要求高的场合很早已经不再使用 MD5。

近年来，对 MD5 的攻击研究取得了一系列成果，使 MD5 即使在商用场合也已不宜使用。2004 年 8 月，在美国加州圣芭芭拉召开的国际密码大会上，中国学者王小云首次宣布了其研究小组近年来的研究成果——对 MD5、HAVAL-128、MD4 和 RIPEMD 等四个著名密码算法的攻击结果。这一研究结果引起了轰动，会议的总结报告写道“我们该怎么办？MD5 被重创了，它即将从应用中淘汰。SHA-1 仍然活着，但也见到了它的末日。现在就得开始更换 SHA-1 了。”2007 年，Marc Stevens，Arjen K. Lenstra 和 Benne de Weger 进一步指出，透过伪造软件签名，可重复性攻击 MD5 算法。研究者使用前缀碰撞法（chosen-prefix collision），使程序前端包含恶意程序，利用后面的空间添上垃圾代码凑出同样的 MD5 散列值。2008 年，荷兰埃因霍芬技术大学科学家成功把 2 个可执行档案进行了 MD5 碰撞，使得这两个执行结果不同的程序被计算出同一个 MD5。2008 年 12 月，在德国柏林举行的“混沌通信”会议上，一些科研人员宣布，他们透过 MD5 碰撞成功生成了伪造的 SSL（安全套接字层）证书，这使得在 https 协议中服务器可以伪造一些根 CA 的签名。这充分说明，对 MD5 的实际攻击已经完全成为可能。

3.5.3　SHA-1

安全散列算法 SHA（Secure Hash Algorithm）是美国国家标准与技术研究院（NIST）公布的安全散列标准 SHS（Secure Hash Standard）中的散列算法。安全散列标准 SHS 于 1993 年 5 月 11 日正式公布后，NIST 又对其做了一些修改。1995 年 4 月 17 日，NIST 正式公布了修改后的 SHS。在新的标准中，将修改后的 SHA 称为 SHA-1，并作为联邦信息处理标准 FIPS 180-1，其产生的消息摘要长度为 160 比特。2002 年，NIST 又公布了 SHA-2，这就是后来的美国联邦信息处理标准 FIPS 180-2。本小节仅介绍有代表性的 SHA-1。

1．算法描述

1）对消息 M 填充

填充消息 M，使其长度恰好为一个比 512 的倍数仅小 64 比特的数。填充方法是附一个 1 在消息后面，后接所要求的多个 0。

2）添加消息长度

在 1）的结果之后，用一个 64 比特的整数表示消息的原始长度（填充字节前消息 M 的长度）使添加后消息长度恰好是 512 比特的整数倍。以上的过程与 MD5 算法是一样的。这

样我们可将消息 M 分为长为 32 比特的一系列子分组 M_0、M_1、…、M_{N-1}，共 N 组。即在每个 512 比特的分组中，含有 16 个 32 比特的子分组，则填充并添加消息长度后的消息 M 共有 N/16 个 512 比特的分组。

3）为五个寄存器赋值

设 A、B、C、D、E 是五个 32 比特的寄存器，其初始值（用十六进制表示）分别为：

A = 67452301

B = efcdab89

C = 98badcfe

D = 10325476

E = c3d2e1f0

4）执行 4 轮操作

对 i = 0 至 N/16-1 执行第（1）步至第（8）步（即对每个 512 比特的分组，分别执行第（1）步至第（8）步）。

（1）对 j = 0 至 15 执行 $X[j] = M[16i+j]$。

（2）对 j = 16 至 79 执行

$$X[j] = (X[j-3] \oplus X[j-8] \oplus X[j-14] \oplus X[j-16]) <<<1。$$

第（1）和（2）步操作相当于将每个 512 比特分组中的 16 个 32 比特的子分组扩展为 80 个 32 比特的子分组。

（3）将寄存器 A、B、C、D、E 中的值分别存储到另外五个寄存器 AA、BB、CC、DD、EE 中，即：

AA = A，BB = B，CC = C，DD = D，EE = E。

（4）执行 Round1。

（5）执行 Round2。

（6）执行 Round3。

（7）执行 Round4。

（8）A = A +AA ，B = B+ BB，C = C+CC，D = D+DD，E = E+EE。

下面对 SHA-1 中的 Round1、Round2、Round3、Round4 做进一步的描述。

Round1、Round2、Round3、Round4 中所使用的函数分别为

$$f_1(X,Y,Z) = (X \wedge Y) \vee (X \wedge Z),$$

$$f_2(X,Y,Z) = X \oplus Y \oplus Z,$$

$$f_3(X,Y,Z) = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z),$$

$$f_4(X,Y,Z) = f_2(X, Y, Z)$$

$$= X \oplus Y \oplus Z。$$

Round1、Round2、Round3、Round4 中所使用的常数（用十六进制表示）分别为

K_1 = 5a827999,

K_2 = 6ed9eba1,

K_3 = 8f1bbcdc,

K_4 = ca62c1d6.

Round1 为：

对 k = 0 至 19 执行

$$TEMP = (A<<<5) + f_1(B,C,D) + E + X[k] + K_1,$$

E = D，D = C，C = (B<<<30)，B = A，A = TEMP。

Round2 为：

对 k = 20 至 39 执行

TEMP = （A<<<5）+ f_2（B,C,D）+E+$X[k]$+K_2，

E = D，D = C，C =（B<<<30），B = A，A = TEMP。

Round3 为：

对 k = 40 至 59 执行

TEMP = （A<<<5）+ f_3（B,C,D）+E+$X[k]$+K_3，

E = D，D = C，C =（B<<<30），B = A，A = TEMP。

Round4 为：

对 k = 60 至 79 执行

TEMP = （A<<<5）+ f_4（B,C,D）+E+$X[k]$+K_4，

E = D，D = C，C =（B<<<30），B = A，A = TEMP。

5）计算消息摘要

在上述算法中，每次循环处理 16 个 32 比特的字，循环的次数为 N/16，最后一次循环结束时，将寄存器 A、B、C、D、E 中的值排列在一起即为 SHA-1 的输出。这就是消息 M 的长度为 160 比特的消息摘要。

图 3-17 说明了 SHA-1 的 4 轮操作过程。

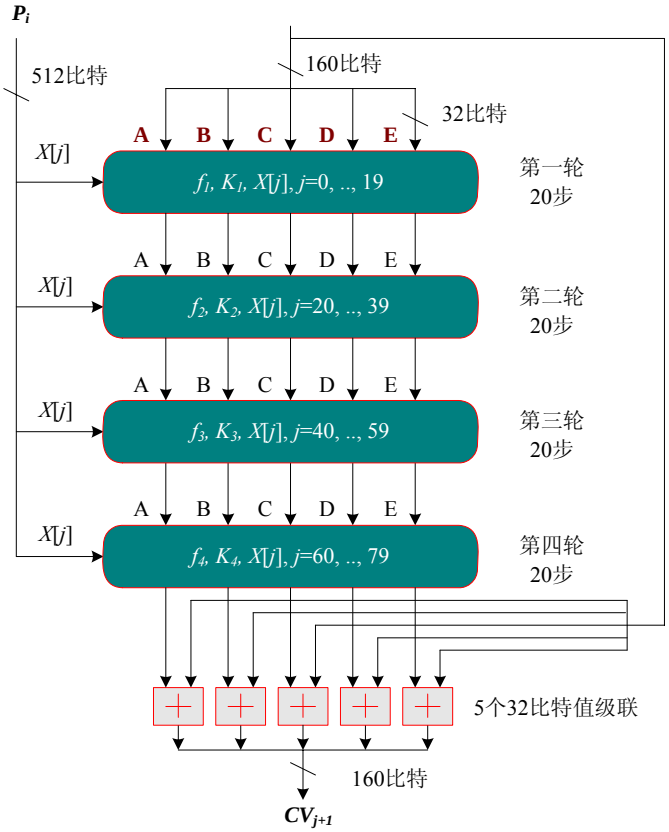


图 3-17　SHA-1 的 4 轮操作过程

图 3-18 进一步说明了在每一轮的变化中，各个寄存器的值的变化过程。

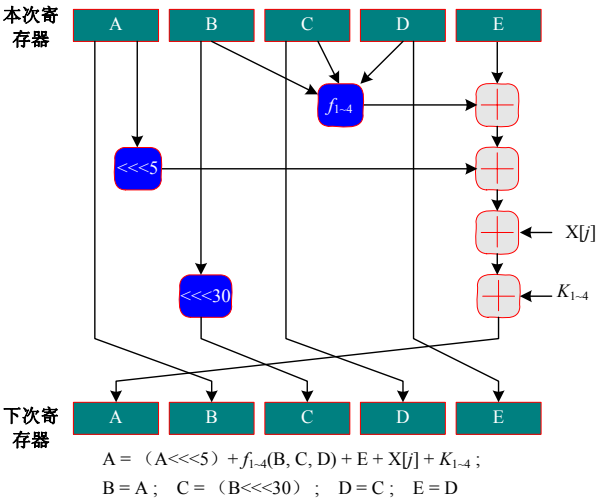


图 3-18　SHA-1 中寄存器值的变化

2．SHA-1 的安全性

2005 年，Rijmen 和 Oswald 发表了对 SHA-1 较弱版本（即 53 次的加密循环而非 80 次）的攻击：在 2^{80} 的计算复杂度之内找到碰撞。2005 年 2 月，中国学者王小云的研究团队发表了对完整版 SHA-1 的攻击，只需少于 2^{69} 的计算复杂度，就能找到一组碰撞（利用暴力搜寻法找到碰撞需要 2^{80} 的计算复杂度）。

鉴于各国科学家们在 SHA-1 算法攻击方面取得的成果，NIST 曾经发表如下声明：“研究结果说明 SHA-1 的安全暂时没有问题，但随着技术的发展，NIST 计划在 2010 年之前逐步淘汰 SHA-1，换用其它更长更安全的算法 SHA-2（如：SHA-224、SHA-256、SHA-384 和 SHA-512）来代替。”根据其声明，2010 年以后美国政府可能仅在下列应用中使用 SHA-1：基于散列的消息认证码（HMAC）、密钥生成函数（KDF）、随机数发生器（RNG）。NIST 鼓励设计者在新的应用和协议中使用 SHA-2。

但由于 SHA-2 与 SHA-1 同属一个散列算法类别，也存在被类似方法攻击的可能，出于谨慎和长远考虑，新的散列函数的研究已经提上了议事日程。NIST 在 2005 年 10 月和 2006 年 8 月举办了两次研讨会，评估了散列函数当前的使用状况，征求了公众对散列函数的策略和准则。两次研讨会召开后，NIST 决定通过公开竞赛，以 AES（高级加密标准）的开发过程为范例，开发一个或多个新的散列算法，从而对 FIPS 180-2 进行增补和修订，预期将在 2012 年完成。NIST 对候选算法提出的可接受的最低标准如下：

（1）算法必须公开并在世界范围内公开专利；

（2）算法必须在广泛的硬件和软件平台上可实现；

（3）算法必须支持 224、256、384 和 512 位消息摘要，支持的最大消息长度至少是 264 位。

NIST 提出的算法评估标准（NIST 将基于以下因素对候选的算法进行比较）如下：

（1）安全性，按以下要素判断：

- 对比其它算法（相同的散列长度），该算法的实际安全性。
- 经过该算法得到的输出和用随机 oracle 模型得到的输出，必须是很难区分的。
- 算法安全所基于的数学基础的稳固性。
- 公众在评估过程中指出的其它安全因素，包括那些能使算法的实际安全性低于提交者所声称的强度的攻击。

（2）花销

- 计算效率。计算效率的评估将在硬件和软件上实施，它涉及到执行时的吞吐量。

NIST 将用最优化的软件，在多种平台上，用多个消息长度对提交的算法进行计算效率的分析。同时也会考虑参赛者本人提交的数据和公众的评论。

- 内存需求。它包括硬件实现时门的数量，软件实现时代码的规模和 RAM 的需求。NIST 将用最优化的软件在多种平台上，用多个消息长度对提交的算法进行内存需求测试。同时也会考虑参赛者本人提交的数据和公众的评论。

（3）算法的实现特征

- 简易性。
- 适应性，即能满足更多用户的需要。“适应性”的例子包括（但不限于）：算法参数化，例如能调整轮数；算法能并行实现，从而达到高效性；算法能在各类平台上安全有效地实现，包括像智能卡一样的受限环境中。

2009 年 2 月，NIST 宣布，其总计收到了 64 个算法，经过评估，51 个算法满足最低要求，这 51 个算法作为候选算法将进入第一轮竞赛。感兴趣的读者可以参考 NIST 的网站了解有关最新动态。

3.6 相关方面的应用

密码技术贯穿于信息安全的全过程，被广泛应用于保护信息安全的各个方面。网络中身份识别、信息存储和传输的加密保护、信息的完整性、信息的不可抵赖性等都要依靠密码技术来实现。除此之外，密码还能够实现访问控制、授权管理、责任认定和网络安全隔离。另外，采用密码保障信息安全与其它方式相比，能够以较少的投入，产生巨大的经济效益和社会效益。

当然，在信息安全中密码不是万能的，但离开密码万万不能。密码技术能够有效实现“进不来、窃不走、看不懂、打不乱、赖不了”的安全目标。但密码技术需要与其它安全技术交流融合，互相渗透，才能提供完整的信息安全解决方案。

作为示例，本小节介绍密码技术在数字签名方面的应用以及公钥基础设施（PKI）技术。这两种应用已经非常广泛，读者会在很多场合遇到。

3.6.1 数字签名

数字签名技术是对数字信息进行签名，它的实现基础是加密技术。

以往的书信或文件是根据亲笔签名或印章来证明其真实性的。但在计算机网络中传送的报文又如何盖章呢？这就是数字签名所要解决的问题。数字签名必须保证以下几点：

（1）接收者能够核实发送者对报文的签名；

（2）发送者事后不能抵赖对报文的签名；

（3）接收者不能伪造对报文的签名。

1．基本原理

大多数数字签名应用都是使用非对称密码算法实现的。在这里我们介绍用非对称加密算法进行数字签名的基本原理：

假设发送者为 A，接收者为 B，设 A 的公开密钥为 PK_A，私有密钥为 SK_A，B 的公开密钥为 PK_B，秘密密钥为 SK_B。

A 用 SK_A 对消息 M 进行以下运算并并发给 B：

$$D_{S_{KA}}(M)$$

$D_{SK_A}(M)$ 就是 A 的数字签名。B 收到 $D_{SK_A}(M)$ 后，用 A 的公开密钥进行运算：

$$E_{PK_A}(D_{S_{KA}}(M)) = M$$

因为除 A 外，没有别人能具有 A 的解密密钥 SK_A，且 A 的公开密钥 PK_A 和私有密钥是成对产生的，所以用 A 的私钥运算后得到密文只有用 A 的公开钥运算才能得到明文信息 M，没有任何密钥通过运算得到明文 M。这样，就证明了这个消息的确来源于 A，A 事后也无法

否认。接收者由于不具备 A 的私钥，其伪造的签名无法被 B 恢复出 M。

同样，设 A 为接收者，B 为发送者，A 也可以利用 PK_B 来恢复被 B 用 SK_B 的消息，从而验证 B 的签名。

下面我们用 RSA 算法来实现数字签名和验证过程。

（1）设计密钥：先选取两个互素的大素数 p 和 q，令 $n=p\times q$，$\varphi(n)=(p-1)(q-1)$，接着寻求整数 e，使 e 与 $\varphi(n)$ 互素。另外，再寻找整数 d，使其满足 $ed \equiv 1 \pmod{\varphi(n)}$，$e$ 和 n 便是公钥，d 是私钥。

（2）设计签名：对消息 M 进行签名，其签名过程是：

$$S = Sig(M) = M^d \pmod{n}$$

（3）验证签名：对 S 按下式进行验证：

$$M' = S^e \pmod{n}$$

如果 $M = M'$，则签名为真。

上述过程与 RSA 加密的相同点是，都使用一对密钥：公钥和私钥。但不同点是，RSA 加密时是用公钥加密，用私钥解密；而 RSA 签名时则是用私钥签名，用公钥验证。

这里给出一个具体的实例说明上述的 RSA 签名和验证过程。

（1）B 选择 $p=11$ 和 $q=13$。

（2）那么，$n=11\times13=143$，$\varphi(n)=10\times12=120$。

（3）再选取一个与 120 互素的数，例如 $e=7$。

（4）找到一个值 $d=103$ 满足 $ed \equiv 1 \pmod{\varphi(n)}$（$7\times103=721$ 除以 120 余 1）。

（5）143 和 7 为公钥，103 为私钥。

（6）B 在一个目录中公开公钥 $n=143$ 和 $e=7$。

（7）现假设 B 想发送消息 85 给 A，他用自己的密钥 $d=103$ 进行签名

$$85^{103} \pmod{143} = 6,$$

于是发送消息 85 和签名 6 给 A。

（8）当 A 接收到消息 85 和签名 6 时，用 B 公开的公钥 $e=7$ 进行验证：

$$6^7 \pmod{143} = 85,$$

与 B 发送的消息一致，于是确定该消息是由 B 所发送，且没有被修改。

事实上，以上的过程只是一种理想的状态，在现实中并不可行。这是由于对整个消息进行签名时速度会非常慢。此外，对于 RSA 算法而言，还存在乘法攻击的可能性，这是由于 RSA 算法中乘幂保留了输入的乘法结构，感兴趣的读者可以参考有关文献，进一步了解 RSA 算法的这一弱点。

因此，发送者在发信前一般使用散列算法求出待发信息的数字摘要，然后用私钥对这个数字摘要而不是待发信息本身进行加密，将加密的结果作为数字签名。发信时，将这个数字签名信息附在待发信息后面，一起发送过去。接收者收到信息后，一方面用发送者的公钥对数字签名解密，得到一个摘要 H；另一方面把收到的信息本身用散列算法求出另一个摘要 H'，再把 H 和 H' 相比较，看看两者是否相同。根据散列函数的特性，我们可以让简短的摘要来“代表”信息本身，如果两个摘要 H 和 H' 完全符合，证明信息是完整的，且发送者不可否认；如果不符合，就说明信息被人篡改了，或者信息不是来自于发送者。

RSA 是一种比较简单的数字签名方案，除此之外还有很多其它的方案。总体而言，在各种数字签名方案中，基于离散对数的数字签名方案和基于大数分解的签名方案是最为常见的两大类。1991 年美国国家标准与技术研究院（NIST）提出了数字签名算法 DSA（Digital Signature Algorithm），用于其数字签名标准 DSS（Digital Signature Standard），这就是一种基于离散对数的方案。此外还有 ElGmal 签名方案、Okamoto 签名方案等都是基于离散对数的。Guillou-Quisquater 签名方案、Fiat-Shamir 签名方案等是基于大数分解的。除此之外，还有

许多其它的签名方案，如盲签名、不可否认签名、防失败签名以及群签名等，感兴趣的读者可以参考有关文献。

2．数字信封

数字签名原理中定义的是对原文做数字摘要并签名，然后传输原文。但在很多场合下，还要求对传输的原文进行保密，即同时实现数字签名和加密。这就涉及到了“数字信封”或“电子信封”的概念，其基本原理是将原文用对称密钥加密传输，而将对称密钥用收方公钥加密发送给对方。收方收到电子信封，用自己的私钥解密信封，取出对称密钥解密得原文。其详细过程如下：

（1）发送方 A 将原文信息进行散列运算，得一散列值，即数字摘要 *MD*；

（2）发送方 A 用自己的私钥 SK_A 对数字摘要 *MD* 进行加密，即得数字签名 *DS*，这里假设使用的非对称算法是 RSA 算法；

（3）发送方 A 用对称算法（例设为 DES 算法）的对称密钥 K_{AB} 对原文信息、数字签名 *DS* 采用对称算法加密，得加密信息 *E*；

（4）发送方用收方 B 的公钥 PK_B，采用 RSA 算法对对称密钥 K_{AB} 加密，形成数字信封 *DE*，就好像将对称密钥 K_{AB} 装到了一个用接收方公钥加密的信封里；

（5）发送方 A 将加密信息 *E* 和数字信封 *DE* 一起发送给接收方 B；

（6）接收方 B 收到数字信封 *DE* 后，首先用自己的私钥 SK_B 解密数字信封，取出对称密钥 K_{AB}；

（7）接收方 B 用对称密钥 K_{AB} 通过 DES 算法解密加密信息 *E*，还原出原文信息、数字签名 *DS*；

（8）接收方 B 用发送方 A 的公钥 PK_A 解密数字签名得到数字摘要 *MD*；

（9）接收方 B 同时将原文信息用同样的散列运算，求得一个新的数字摘要 *MD'*；

（10）接收方 B 将两个数字摘要 *MD* 和 *MD'*进行比较，验证原文是否被修改。如果二者相等，说明数据没有被篡改，是保密传输的，签名是真实的；否则拒绝该签名。

经过以上过程，就做到了敏感信息在数字签名的传输中不被篡改，未经认证和授权的人，看不见原数据，起到了在数字签名传输中对敏感数据的保密作用。这个过程如图 3-19 所示。

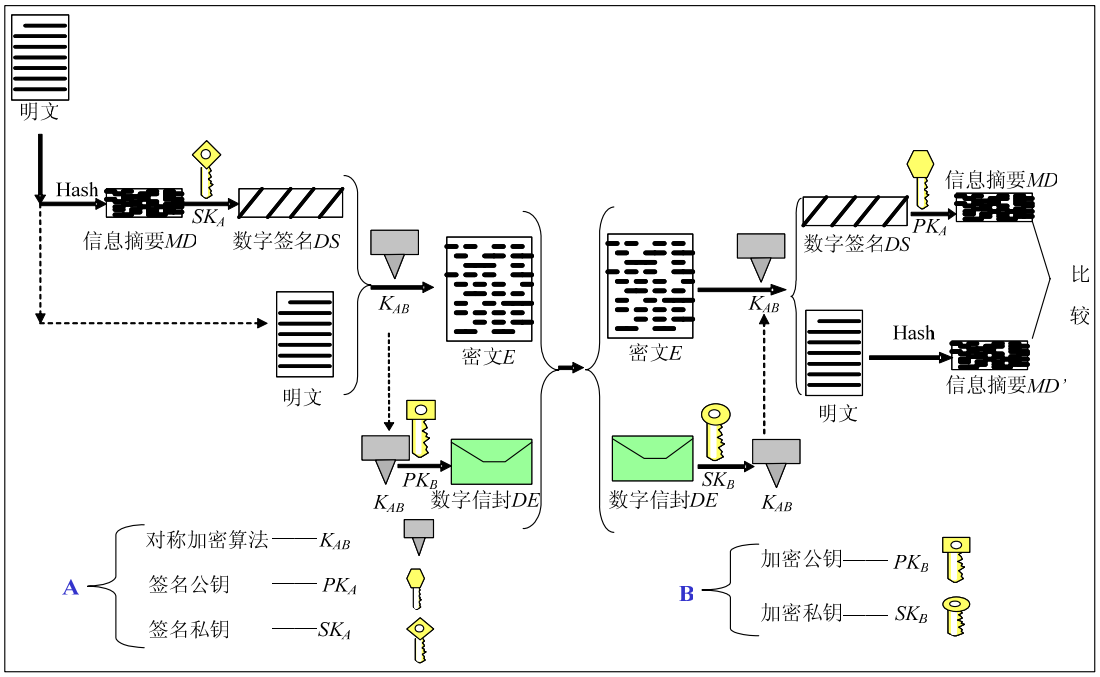


图 3-19　数字信封示意图

3．数字签名与电子签名的关系

为了促进我国信息化发展，保护电子商务和电子政务中各方当时人的合法权益，构建诚信体系，全国人大常委会于 2004 年 8 月通过了《中华人民共和国电子签名法》，2005 年 4 月 1 日正式实施，这是我国信息化领域的首部法律。电子签名和数字签名的内涵并不一样，数字签名是电子签名技术中的一种，不过两者的关系也很密切。

要理解什么是电子签名，需要从传统手工签名或盖印章谈起。在传统商务活动中，为了保证交易的安全与真实，一份书面合同或公文要由当事人或其负责人签字、盖章，以便让交易双方识别是谁签的合同，保证签字或盖章的人认可合同的内容，在法律上才能承认这份合同是有效的。而在电子商务的虚拟世界中，合同或文件是以电子文件的形式表现和传递的。在电子文件上，传统的手写签名和盖章是无法进行的，这就必须依靠技术手段来替代。能够在电子文件中识别双方交易人的真实身份，保证交易的安全性和真实性以及不可抵赖性，起到与手写签名或者盖章同等作用的签名的电子技术手段，称之为电子签名。

从法律上讲，签名有两个功能：即标识签名人和表示签名人对文件内容的认可。联合国贸发会的《电子签名示范法》中对电子签名作如下定义：“指在数据电文中以电子形式所含、所附或在逻辑上与数据电文有联系的数据，它可用于鉴别与数据电文相关的签名人和表明签名人认可数据电文所含信息”；在欧盟的《电子签名共同框架指令》中就规定：“以电子形式所附或在逻辑上与其它电子数据相关的数据，作为一种判别的方法”称电子签名。我国《中华人民共和国电子签名法》对电子签名的定义是：“指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。”

实现电子签名的技术手段有很多种，除数字签名外，还可以使用以下几种方法：

（1）手写签名或图章的模式识别。即将手写签名或印章作为图像，用光扫描经光电转换后在数据库中加以存储，当验证此人的手写签名或盖印时，也用光扫描输入，并将原数据库中的对应图像调出，用模式识别的数学计算方法，进行二者比对，以确认该签名或印章的真伪。这种方法曾经在银行会计柜台使用过，但由于需要大容量的数据库存储和每次手写签名和盖印的差异性，证明了它的不可实用性，这种方法也不适用于互联网上传输。

（2）生物识别技术。这是一种利用人体生物特征进行身份认证的技术。生物特征是一个人与他人不同的唯一表徵，它是可以测量、自动识别和验证的。生物识别系统对生物特征进行取样，提取其唯一的特征进行数字化处理，转换成数字代码，并进一步将这些代码组成特征模板存于数据库中，人们同识别系统交互进行身份认证时，识别系统获取其特征并与数据库中的特征模板进行比对，以确定是否匹配，从而决定确定或否认此人。生物识别技术主要有指纹识别、视网膜识别、声音识别等技术。

2005 年 7 月，北京市海淀区人民法院审理了一起案件，韩某两次发手机短信给朋友杨某，向其借钱应急，杨某根据韩某的要求汇钱之后未要求韩某签订借条，后杨某多次催要未果，于是起诉至法院，并提交了银行汇款单存单两张。但韩某却称这是杨某归还以前欠款所陈生的汇款单存单。庭审中，杨某向法庭提交了其手机中留存的短信息内容。后经法官核实，杨某提供的发送短信的手机号码拨打后接听者是韩某本人，而韩某本人也承认该手机号码为自己所有。法院经审理认为，依据《中华人民共和国电子签名法》中的规定，经法院对杨某提供的手机短信息生成、储存、传递数据电文方法的可靠性、保持内容完整性方法的可靠性、用以鉴别发件人方法的可靠性进行审查，可以认定该手机短信息内容作为证据的真实性。经对照手机短信息内容中载明的款项往来金额、时间与银行个人业务凭证中体现的杨某给韩某汇款的金额、时间，法院认定手机短信息可以认定为真实有效的证据，予以采纳。这个案例说明，只要符合了《中华人民共和国电子签名法》中规定的书面形式、原件形式、文件保存要求以及证据效力，都可以作为获得法律承认的电子签名，包括手机短信息。

当然，目前比较成熟的，世界先进国家普遍使用的电子签名技术还是“数字签名”技术。

由于保持技术中立性是制订法律的一个基本原则，目前还没有任何理由说明公钥密码理论是制作电子签名的唯一技术，因此法律中规定了更一般化的“电子签名”概念以适应今后技术的发展。大多数情况下，人们提到的电子签名一般指的都是“数字签名”。

3.6.2 公钥基础设施（PKI）

大多数公钥密码系统都容易受到“中间人”（man-in-the-middle）攻击。例如考虑 A 和 B 进行通信的情况。假设 C 能够拦截公钥的交换，C 可以向 A 发送他自己的公钥，但故意将其表示成 B 的公钥；然后，他还可以向 B 发送了自己的公钥，故意表示成 A 的公钥。那么现在 C 便可以拦截 A 和 B 之间的所有通信了。如果 A 向 B 发送了一条加密的消息，由于实际上使用的是 C 的公钥，C 获得消息后解密并进行存储，这样他就可以稍后读这条消息了。这之后，他使用 B 的公钥加密其篡改后消息，继续将其发送给 B。B 获得消息后能够为其译码，但不知道它实际上是来自 C 而非 B。

上面的问题的实质是 A 没办法确定他得到的密钥是否真的属于 B。公钥是公开的，因此不需确保秘密性。然而，却必须确保公钥的真实性和完整性，绝对不允许攻击者替换或篡改用户的公钥。如果公钥的真实性和完整性受到危害，则基于公钥的各种应用的安全将受到危害。这实际上是一种信任问题。A 和 B 可以相互信任，但他们如何能够知道与其通信的人到底是不是对方所声称的人呢？他们如何才能确保所收到的公钥真正属于他们要发消息的人呢？在一个小的团体内部，这个问题很容易解决，但在互联网这样的环境中，显然需要建立一种信任机制。

这就是公钥基础设施（PKI）要解决的核心问题。它是一种可信的第三方，保持着对每个用户的密钥的跟踪，其两种基本操作是证明（将公钥值与所有者绑定的过程）和验证（验证证书依然有效的过程）。当前，PKI 已经成为一种用公钥概念和技术实施和提供安全服务的具有普适性的安全基础设施，以核心的密钥和证书管理服务为基础，PKI 及其相关应用保证了网上数字信息传输的保密性、完整性、真实性和不可否认性。

在电子商务应用环境中，交易双方互不隶属，仅仅依靠交易双方无法实现信任凭证，必须要依靠一个交易双方都认可的可信第三方机构来提供信任证明，PKI 便是在交易双方都无法信任的情况下提供了第三方信任机制。但是，特别需要引起注意的是，社会活动中还有很多不需要引入第三方信任的场合，例如在一个单位的内部。在这种情况下，虽然也需要使用证书与公钥技术，但不必引入 PKI 架构，否则便可能会带来巨大的资源浪费。

1．PKI 的组成和功能

从广义上讲，PKI 体系是一个集网络建设、软硬件开发、信息安全技术、策略管理和相关法律政策为一体的大型的、复杂的、分布式的综合系统。我们在这里仅讨论狭义范围的 PKI。一般而言，一个比较完整的 PKI 至少应包括以下 7 个部分的内容。

1）认证机构（CA）

PKI 的核心是信任关系的建立和管理。假设甲国公民 A 和乙国公民 B 互相不认识，更不信任对方，如果存在公正的可信任的第三方 C（例如护照签发机关），使 A 和 B 都直接信任 C，那么此时公民 A 和 B 就可以信任对方了，这就是所谓的第三方信任。由此可以看出，在建立第三方信任时，公正、可信任的第三方 C 对于信任关系的建立和巩固起到至关重要的作用。而认证机构（CA）就扮演着一个具有权威性的第三方角色，是 PKI 的主要组成部分之一，它的核心职责就是完成证书的管理（证书的概念请参考后面的介绍）。CA 使用自己的私钥对 RA（证书注册机构）提交的证书申请进行签名，来保证证书数据的完整性，任何对证书内容的非法修改，都会被用户使用 CA 的公钥进行验证而发现，这是证书合法性的基础。

广义的认证中心还应包括证书注册机构（RA），它是数字证书的申请注册、签发和管理的机构，是 CA 和最终用户之间的接口。这项功能通常由人工完成，也可以由机器自动完成。

在实际应用中，有些 PKI 的 RA 功能并不独立存在，而是合并在 CA 之中。

对 CA 最重要的事情是自己的一对密钥的管理，CA 的私钥必须高度保密，以防止他人伪造证书。CA 的公钥在网上公开，因此整个网络系统必须保证完整性。CA 在为用户颁发数字证书时，用户的公钥有两种产生的方式：一是用户自己生成密钥对，然后将公钥以安全的方式传送给 CA，该过程必须保证用户公钥的验证性和完整性；二是 CA 替用户生成密钥对，然后将其以安全的方式传送给用户。该方式下由于用户的私钥为 CA 所产生，所以对 CA 的可信性有更高的要求。

2）证书和证书库

证书是数字证书或电子证书的简称，是构成 PKI 的基本元素。它是参与网上信息交流及商务交易活动的各个实体（例如持卡人、企业、商家、银行等）的身份证明，证明该用户真实身份和公钥的合法性，以及该用户与公钥的匹配关系。它相当于护照，而且是一种“电子护照”。

证书库是网上的一种公共信息存储仓库，用于存储、撤销 CA 已签发证书及公钥，可供公众进行开放式查询。一般而言，查询的目的有两个：一是获得商务活动时对方的公钥，以便加密数据并通过网络传送，完成商务活动；二是验证对方的证书是否已经作废，即该证书是否已经不再被使用。

3）密钥备份及恢复系统

密钥备份及恢复是 PKI 密钥管理的重要内容之一。如果某用户由于某种原因不慎丢失解密密钥，则意味着加密数据的完全丢失，那么就有可能造成合法的数据大量丢失，导致不可挽回的巨大经济损失。为了避免灾难的发生，PKI 提供了密钥备份及恢复系统。当用户证书生成的同时，解密密钥就被 CA 备份并存储起来，当需要恢复时，用户只需要向 CA 提出申请，CA 就会为用户自动进行恢复。当然，签名私钥为确保其惟一性而不能够作备份和恢复。

4）密钥和证书的更新系统

与日常生活中我们使用的各种各样的身份证件相似，证书也有自己的使用期限，而且由于某种原因在有效期内也可能作废，例如密钥丢失、用户的个人身份信息发生改变、CA 对用户不再信任或者用户对该 CA 不再信任等各种情况。为此，证书和密钥必须要有一定的更新频率。证书的更新一般可以有 3 种方式：更换一个或多个主题的证书；更换由某一对密钥签发的所有证书；更换某一个 CA 签发的所有证书。即使在用户正常使用证书的过程中，PKI 也会自动不定时地到目录服务器中检查证书的有效期，当有效期将满时，CA 会自动启动更新程序，将旧证书列入作废证书列表（俗称黑名单），同时生成一个新证书来代替原来旧证书，并通知用户。

5）证书历史档案

经过若干时间以后，每一个用户都会形成多个旧证书和一个当前证书。这些旧证书及相应的私钥就组成了用户密钥和证书的历史档案。记录整个密钥历史是非常重要的。例如，某用户几年前用自己的公钥加密的数据或者其他人用自己的公钥加密的数据就无法用现在的私钥解密，那么该用户就必须提出申请，从他的密钥历史档案中，查找到当年使用的私钥来解密这些数据，保证数据使用的连贯性。

6）应用接口系统

为方便用户操作，解决 PKI 的应用问题，一个完整的 PKI 还必须提供良好的应用接口系统，以实现数字签名、加密传输数据等安全服务，使得各种应用能够安全、一致、可信地与 PKI 交互，确保安全网络环境的完整性、易用性和可信度。

7）交叉认证

交叉认证是为了解决公共 PKI 体系中各个 CA 机构互相分割互不关联的“信任孤岛”问

题，实现多个 PKI 域之间互联互通，从而满足安全域可扩展性的要求。目前，比较典型的交叉认证的模型有：树状认证模型、网状认证模型、桥式模型、信任列表模型、相互承认模型等。

2．数字证书

如前所述，在 PKI 系统中，数字证书简称为证书。它是一个数据结构，是一种由一个可信任的权威机构签署的信息集合。PKI 系统中的公钥证书是一种包含持证主体标识、持证主体公钥等信息，并由可信任的 CA 签署的信息集合，主要用于确保公钥与用户的绑定关系，它的持证主体可以是人、设备、组织机构或其它主体。

任何一个用户只要知道签证机构 CA 的公钥，就能检查对证书的签名的合法性。如果检查正确，那么用户就可以相信那个证书所携带的公钥是真实的，而且这个公钥就是证书所标识的那个主体的合法的公钥。

由于 PKI 适用于异构环境中，所以证书的格式在所使用的范围内必须统一。目前应用最广泛的证书格式是国际电信联盟 ITU 提出的 X.509 版本 3 格式。X.509 标准最早于 1988 年颁布，在此之后又于 1993 年和 1995 年进行过两次修改。此后，互联网工程任务组（IETF）针对 X.509 在互联网环境的应用，颁布了一个作为 X.509 子集的 RFC2459。从而使 X.509 在 INTERNET 环境中得到广泛应用。

一个标准的 X.509 数字证书包含以下一些内容。

- 证书的版本信息。
- 证书的序列号，每个证书都有一个惟一的证书序列号。
- 证书所使用的签名算法。
- 证书的发行机构名称，命名规则一般采用 X.500 格式。
- 证书的有效期。
- 证书所有人的名称，命名规则一般采用 X.500 格式。
- 证书所有人的公开密钥。
- 证书发行者对证书的签名。

X.509 证书的标准格式如图 3-20 所示。

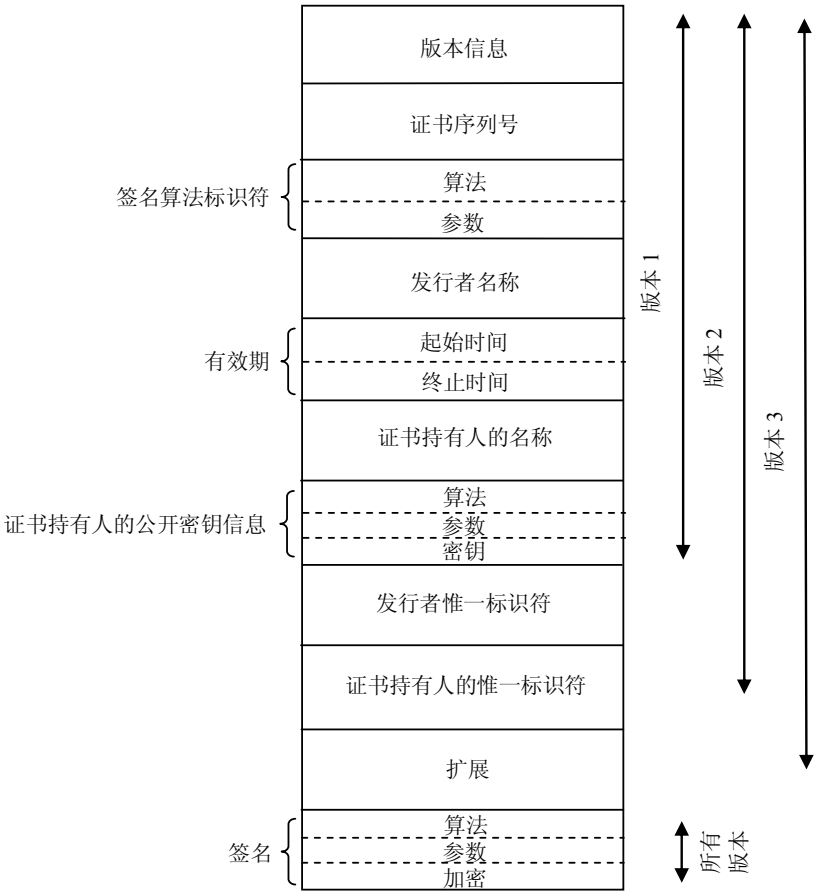


图 3-20　X.509 证书的标准格式

我国于 2006 年 8 月发布了国家标准《信息安全技术 公钥基础设施 数字证书格式》，这一标准主要根据 RFC2459 制定，并结合我国数字证书应用的特点进行了相应的扩充和调整。

3．PKI 应用示例

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。当然，作为一种基础设施，PKI 的应用范围非常广泛，并且在不断发展之中，这里给出 PKI 在安全电子邮件中的应用示例。

电子邮件的方便快捷特性已使其成为重要的沟通和交流工具，但目前的电子邮件系统却存在着较大的安全隐患：邮件内容以明文形式在网上传送，易遭到监听、截取和篡改；无法确定电子邮件的真正来源，也就是说，发信者的身份可能被人伪造。因此，安全电子邮件协议 S/MIME（安全/多用途互联网邮件扩展，The Secure Multipurpose Internet Mail Extension）应运而生。S/MIME 为电子邮件提供了数字签名和加密功能，其实现需要依赖于 PKI 技术。

目前，S/MIME 已经被广泛的应用于各种客户端和平台，大多数电子邮件客户端软件都支持的 S/MIME 协议的最新版本（第三版），因此大多数不同的电子邮件客户程序彼此之间都可以收发安全电子邮件。

Outlook Express 是户常用的客户端电子邮件收发软件，能够自动查找安装在计算机上的数字证书，将这些证书同邮件账户相绑定，并自动将别人发送的数字证书添加到通讯簿中。

在使用 Outlook 安全电子邮件功能之前，用户需要有自己的数字标识。数字标识可以从证书颁发机构 CA 那里获得，它包含一个私钥（该私钥一直保留在用户的计算机上），以及一个证书（含有公钥）。

为了发送签名邮件，用户必须有自己的数字证书；为了发送加密电子邮件，用户需要有收件人的数字证书。获得收件人数字证书的方法可以是让对方发送带有其数字签名的邮件，

将该邮件打开后，在右边会看到对方的证书标志，单击该标识，找到“安全”项，单击“查看证书”按钮，可以查看“发件人证书”；单击“添加到通讯簿”按钮后，在通讯簿中保存发件人的加密首选项，这样对方数字证书就被添加到通讯簿中了。有了对方的数字证书后，就可以向对方发送加密邮件。

本章小结

本章围绕一些主要的密码算法及其应用作了介绍。密码技术包含很多知识，对数学基础也有一定的要求，在一个章节中全面介绍密码技术是不可能的，而且这也超出了本书的目标。本章以密码技术概述为切入点，重点介绍了分组密码、公钥密码、散列函数中几个著名的算法，并在最后给出了有关应用示例。没有接触过密码知识的读者，只要耐心阅读，即使不参考其它文献，也可以掌握这些算法的主要内容。但介绍这些算法本身并不是本章的目的，而是旨在使读者对密码技术增加更多的感性认识，并能够从这些感性认识上升到对信息安全技术体系的更深层次的理解，从而有利于今后更系统和全面地学习信息安全专业知识。

本章的内容包括以下方面：

（1）密码技术概述

一个密码系统，通常由明文空间、密文空间、密钥空间、加密算法和解密算法组成。根据密码体制所使用的密钥，可以将其分为两类，即单钥密码体制与双钥密码体制。单钥密码体制又进一步分为流密码（也称序列密码）和分组密码。单钥密码体制和双钥密码体制各有优缺点，在安全通信系统中往往承担不同的角色。

密码攻击方法主要有穷举攻击、统计分析攻击和数学分析攻击。根据密码分析者可利用的数据来分类，密码攻击还可以分为唯密文攻击、已知明文攻击、选择明文攻击和选择密文攻击。

（2）流密码

流密码又称为序列密码，其基本思想是对明文符号序列用密钥流进行加密，产生密文序列。根据密钥流与明文符号的关系，流密码又分为同步流密码和自同步流密码。线性反馈移位寄存器 LFSR 是构造密钥流生成器的重要部件之一，是深入掌握流密码所需了解的必备知识，限于篇幅，本章没有对此展开讨论。

（3）分组密码

分组密码的结构从本质上说都是基于一个称为 Feistel 网络的结构，其思想实际上是 Shannon 提出的利用乘积密码实现混淆与扩散思想的具体应用。分组密码有四种工作模式：电子密码本模式（ECB）、密码分组链接（CBC）模式、密文反馈（CFB）模式和输出反馈（OFB）模式。

DES 算法是本章介绍分组密码时的重点。虽然目前 DES 算法已经被淘汰，但它对于推动密码理论的发展和应用起了重大作用，对于掌握分组密码的基本理论设计思想和实际应用仍然有着重要的参考价值。除 DES 算法外，还简单介绍了 IDEA 算法、AES 算法和 SMS4 算法，掌握这些算法需要较多的数学知识，建议感兴趣的读者参考相关文献。

（4）公钥密码

在公钥密码中，最著名也是应用最广的密码算法是 RSA 密码算法和椭圆曲线密码算法。RSA 算法是本章介绍公钥密码时的重点，欧拉定理是这一算法的数学基础，读者应该熟练掌握其数学原理以及算法的实现过程。RSA 的安全性基于大整数因子分解问题的难解性。目前，1024 比特的 RSA 算法的安全性已经受到质疑，很多标准中都要求使用 2048 比特的 RSA 算法。

除 RSA 算法外，本章还介绍了椭圆曲线密码算法。椭圆曲线密码算法在当前十分流行，但掌握该算法需要一定的数学基础，因此本章没有将其作为重点，读者可以从相关文献中了

解更详细的内容。

（5）散列函数

散列函数在信息安全领域具有重要应用，它是实现数据完整性和身份认证的核心技术，本章介绍了常用的 MD5 算法和 SHA-1 算法，包括算法的详细描述以及有关安全性的说明。

MD5 算法不但从理论上而且从实际操作上被证实很不安全，目前已经不再使用。人们对 SHA-1 算法的攻击也取得了一定的成果，因此美国计划在 2010 年前淘汰 SHA-1，目前正在全球范围内征求更安全的散列算法。

（6）相关应用

本章介绍了密码技术在数字签名方面的应用以及公钥基础设施（PKI）技术。数字签名方案比较多，本章仅以 RSA 算法为例介绍了数字签名的基本原理，还介绍了能够同时实现数字签名和加密功能的“数字信封”技术，此外还结合《中华人民共和国电子签名法》，说明了数字签名与电子签名之间的区别和联系。

在 PKI 部分，本章介绍了；PKI 的基本组成和功能，说明了数字证书的标准格式，并以安全电子邮件为例介绍了 PKI 在实际生活中的应用。

习题

1．密码学经过了几个发展阶段?

2．DES 密码体制中的 f 函数如何将 32 比特扩展成 48 比特？

3．如果输入为“Alice just do it”，第一阶段使用的密钥为 01 01 01 01 20 20 20 20 03 03 03 03 60 60 60 60，那么第一阶段的 AES 输出是什么？

4．假设 AES 的密钥是 30014fd1 69e31044 1782e4b1 23aa4018，第一轮的密钥是什么？

5．概述公钥密码产生的原因。它有哪些优势和不足？

6．在一个 RSA 加密的系统中，假如截获了一个密文 $C = 10$，它对应的公钥是 $e = 5$，$n = 35$，请问明文是什么？

7．设 p = 43，q = 59，取 e = 13，d 值。

8．为了加强 RSA 的安全性，对 p 和 q 的选取有哪些要求？

9．散列函数为什么可以用于对消息的完整性进行验证？

10．考虑用公钥加密算法构造散列函数，设算法是 RSA，将消息分组后用公开钥加密第一个分组，加密结果与第二个分组异或后，再对其加密，一直进行下去。设一消息被分成两个分组 B1 和 B2，其杂凑值为 H（B1，B2）= RSA（RSA（B1）B2)。证明对任一分组 C1 可选 C2，使得 H（C1，C2）= H（B1，B2）。证明用这种攻击法，可攻击上述用公钥加密算法构造的散列函数。

11．数字签名的基本原理是什么？

12．概述数字信封的应用过程。

13．PKI 应用在一种什么样的信任环境下？它由哪些部分组成？

第 4 章　信息系统安全

本章要点

- BLP 模型
- Biba 模型
- 安全操作系统主要安全技术
- 安全数据库主要安全技术
- 骨干网安全技术要求

4.1　信息系统安全模型

信息系统安全模型也称为信息系统安全策略模型。安全策略在本质上可以是非形式化的，也可以是形式化的。安全策略针对保密性、完整性和可用性的具体需求而提出，并通过访问控制机制而实现。形式化的安全策略一般基于强制访问控制机制来实现。

本节介绍几个典型的形式化安全策略模型，分别是 BLP 保密性安全策略模型、Biba 完整性安全策略模型以及 BLP 模型和 Biba 模型结合的二维安全策略模型，并简单介绍了其它一些有一定影响的安全策略模型。

4.1.1　BLP 安全策略模型

Bell-Lapadula 安全模型，简称 BLP 安全模型，是第一个有数学基础的访问控制模型，也是最著名的安全策略模型。它是由 Bell 和 LaPadula 在 1973 年提出的，Denning 则于 1975 年对 BLP 模型给出了一个基于格的严格数学描述。该模型影响了许多其它模型的发展，甚至很大程度上影响了计算机安全技术的发展。

BLP 安全模型中结合了强制型访问控制和自主型访问控制，我们在这里主要讨论 BLP 安全策略模型的强制访问控制部分。

BLP 模型是从军队保密需求而来的。在现实世界中，保密文档一般需要划分密级，假设一个部门的文档其密级由高到低分为绝密、机密、秘密和公开四类，则保密需求就是高密级的信息不能流向低密级的文档。BLP 安全模型的目的就是实现这一信息流安全策略。

上述的密级划分是一种线性的等级分类，BLP 模型还用一种非等级类别与等级分类组合起来，作为系统中主客体的安全标识，并依据这些安全标识来执行强制访问控制操作。所谓非等级的安全类别，也称为范畴，简言之就是对主客体所处的部门的一种描述。为什么需要用非等级类别与等级分类组合来作为主客体的安全标识呢？这在现实生活中很容易找到例证：一个人也许拥有很高的密级，但他不一定允许查阅不属于其工作范围的其他部门的低密级的信息，这就是著名的“应需可知”（need-to-know）的原则。

信息系统中的所有实体都可以分为主体和客体。所谓主体，就是系统中具有主动性的实体，如用户，进程等等，它们可以主动发起操作。所谓客体，则是被动的、作为操作对象的实体，如文件，存储设备等，我们可以把它们看作是存储信息内容的容器。访问是主体对客体的读、写、执行等操作，它会导致信息在主客体之间流动。权限则规定了特定主体对特定客体能够做何种访问。

BLP 模型的强制访问控制遵循两个基本安全条件：简单安全条件和*-属性（星属性）。简单安全条件规定一个主体可以读一个客体的条件是，仅当主体保密级别不低于客体的保密

级别，且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别。*-属性规定一个主体可以写一个客体的条件是，仅当主体保密级别不高于客体的保密级别，且主体安全级中的非等级类别包含于客体安全级中的非等级类别。

BLP 模型的强制访问控制规则实际上是一种信息流策略。在一个系统中，信息可以被认为是从一个客体流到另一个客体，而客体间的信息流动则可以看作是通过主体的读写操作实现的。如果系统中所有访问都遵循 BLP 模型的两条规则时，可以证明，信息将不会从高安全级别的客体流到低安全级别的客体中。

BLP 模型中，安全标识与其间的支配、包含关系形成一个数学上的有限格，BLP 模型的两条规则也可以转化为格中信息的单向流动规则。通过格模型，可以形式化地描述 BLP 模型的安全策略。Biba 模型、中国墙模型等也可以通过有限格来描述，这些模型均属于基于格的访问控制模型，简称 LBAC 模型。

BLP模型实现了一个单向的信息流策略，合法的信息流从低安全级别主体/客体流到高安全级别的主体/客体，逆向的信息流动是被禁止的。但是，实际信息系统中，经常有逆向信息流动的实际需求，如上级向下级发布通知，下达命令等等。在工程中，逆向信息流一般都是通过划定可信主体，并授予其特权来实现。

4.1.2 Biba 安全策略模型

Biba模型是一个针对完整性安全需求的模型。1977年，Biba对系统的完整性进行了研究，他提出了三种策略，其中一种是Bell-Lapadula模型在数学上的对偶。

Biba模型隐含地融入了“信任”这个概念。事实上，用于衡量完整性等级的术语是“可信度”。例如，一个进程所处等级比某个客体的等级要高，则可以认为进程比该客体更“可信”。

Biba模型用线性的完整性等级标识主体和客体，其访问规则为：

（1）当主体完整性级别低于客体完整性级别时，主体可以读客体。

（2）当主体完整性级别高于客体完整性级别时，主体可以写客体。

程序执行是一种常见的对完整性影响较大的行为，但是在关于 Biba 完整性模型的学术文章中，对其有两种观点。一种是认为只有当主体的级别大于执行程序的级别时，主体才能执行程序；另一种观点则不对程序执行做特殊考虑，程序执行前，需要读入执行程序文件，则对这一行为按照读客体来控制。此时，主体能够执行的程序，其在磁盘上存储的文件必然是级别不低于它的执行程序文件。

这两个观点似乎相互矛盾，但实际上是因为双方考虑角度不同。第一种观点把执行程序看作是另一个主体，主体执行程序的过程实际上是主体生成了另一个主体的过程，而执行程序的行为影响的是所执行程序的完整性，因此，主体的完整性级别要高于执行程序的完整性级别，防范低完整性的主体影响执行程序。而第二种观点则把执行程序在磁盘上的存储对象当作客体，当主体读入客体后，执行该客体的行为是原有主体行为的延伸，而读入客体的行为影响的是主体的完整性。因此，主体的完整性级别要低于执行程序文件的完整性级别，防范低完整性的执行程序文件影响主体的完整性。

依据这两个观点来标识执行程序时，按照第一种观点，我们标识的是执行程序本身，控制的行为是执行这个动作，执行程序的安全级别也是根据执行程序的运行情况来确定的；按照第二种观点，我们标识的是执行程序文件，控制的行为是读入执行程序文件这个动作，其安全级别是根据这些数据的来源而确定的。因此，这两种观点实际上并没有矛盾之处。

4.1.3 二维安全策略模型

BLP 模型是一个保密性模型，Biba 模型则是一个完整性模型，因此，一个很自然的想法就是把 BLP 模型和 Biba 模型结合起来，实现一个保密性和完整性兼顾的强制访问控制模型。但是，简单地将二者结合起来，将令信息只能在单一的安全等级之间流动，使系统的不

同安全等级形成信息孤岛。

为了解决这一问题，需要让不同保密级别和完整级别之间的信息能够互相流动。实际上，高保密级别客体存放的信息流到低保密级别，未必会导致泄密事件。因为高保密级别客体可以接受所有低于它的保密级别的信息，因此，我们可以把高保密级别客体中存放的信息看作是不同保密级别信息的混合，如果从高保密级别的客体流向低保密级别的客体中的信息中，只包含低保密级别的信息内容，那么这种逆向信息流动并不会泄密。对完整性也有类似的结论。

因此，我们可以用一种保密性和完整性结合的二维安全标识来标记系统中的主体和客体，将既符合 BLP 模型规则，也符合 Biba 模型规则的访问行为定义为正常访问行为，可以直接放行，对违反规则的访问行为，则需通过保密性检查和完整性检查，如可确认访问导致的信息流中不含有影响保密性和完整性的内容，则也可以允许。图 4-1 可以说明二维安全策略模型的信息流向：

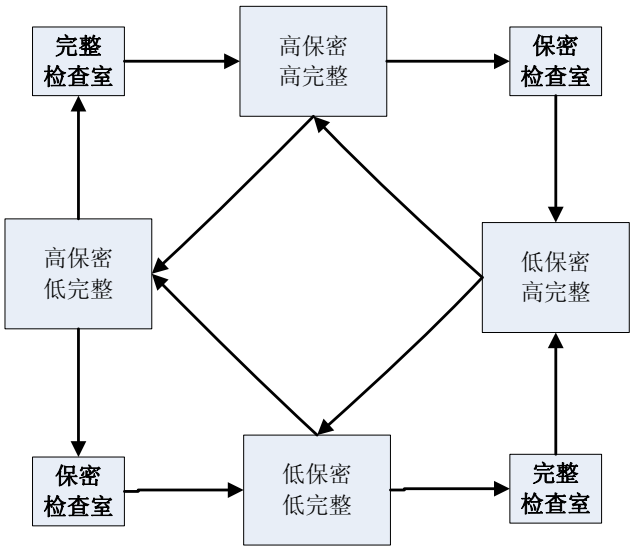


图 4-1　二维安全模型基本安全策略信息流向图

实际工作中，我们一般是通过标识和辨别来实现保密检查和完整性检查。标识是将实体中不同安全级别的信息分别标识，在进行逆向信息操作时，可以通过对标识的检查来确定传递的信息符合安全要求。标识可以根据信息的来源添加，并通过密码学技术保证信息的完整性和标识的不可篡改。辨别则是对逆向信息流中的信息进行内容检查，确定这些信息中不含高保密级别的内容或低完整级别的内容。

对高保密级别内容的辨别方法和对低完整级别内容的辨别方法区别很大，对高保密内容的检查主要是对敏感信息的识别，难以找到固定的方法，在一些场合，可能还需要依赖检查人员的主观判断。对低完整内容的检查主要是数据完整性方面的检查以及恶意代码的识别，在对恶意代码主动识别存在困难的场合，一种比较简单的方法是规定高完整性内容的安全数据格式，通过格式检查来实现低完整性内容的识别。如可以规定高完整级别的数据使用格式为 XML 等安全格式，把低完整级别 word 文档转换为 xml 格式存储后提升为高完整级别，以避免 Word 文档中可能存在的宏病毒。

4.1.4　其它安全策略模型

在本小节，简单介绍 clark-wilson 模型、中国墙模型和 RBAC 模型。在本小节的后一节，还将介绍当前安全模型面临的挑战。

1．clark-wilson 模型

clark-wilson 模型是 1987 年，由 David Clark 和 David Wilson 开发的一种完整性模型，

它以事物处理为基本操作，比较符合商业系统的建模。

商业系统中最关键的问题是：系统数据的完整性以及对这些数据操作的完整性。Clark-wilson 模型将从属于其完整性控制的数据定义为约束型数据项，而不从属于完整性控制的数据为非约束型数据项。另外，模型还定义了两组过程，一组是完整性验证过程，它检验约束型数据项是否符合完整性约束，另一组过程是转换过程，它们将系统数据从一个有效状态转换为另一个有效状态。根据一系列证明规则和实施规则，来确保系统的完整性。

Clark-wilson 模型将证明规则和实施规则区分开来，证明规则需要外界介入，要假设某些东西是可信的，其证明过程一般比较复杂，同时容易出错或不完整。但这个模型明确地进行了假设，而 Biba 模型没有证明规则，只能通过“可信”的断言来保证系统的操作遵守模型的规则。

2．中国墙模型

中国墙模型是一种同等地考虑保密性与完整性的安全策略模型。该策略模型主要解决商业中的利益冲突问题。中国墙模型通常用于股票交易所或者投资公司的经济活动等环境中，在这种环境下，中国墙模型的目标就是防止利益冲突的发生，例如，当交易员代理两个客户的投资，并且这两个客户的最大利益相冲突时，交易员就可能帮助其中一个客户盈利，而导致另一个客户的损失。

中国墙模型用下面的定义抽象描述了这种情况：

（1）数据库的客体是指与某个客户相关的信息条目。

（2）客户数据集（CD）包含了与某个客户相关的若干客体。

（3）利益冲突（COI）类包含了若干相互竞争的客户的数据集。

定义 PR（S）是主体 S 曾经读取过的客体集合，则中国墙模型的策略可以用下面的 CW-简单安全条件来描述：

CW-简单安全条件：S 能读取 O，当且仅当以下任以条件满足：

（1）存在一个 O’，它是 S 曾经访问的客体，且 CD（O’）＝CD（O）.

（2）对于所有的客体 O’，若 O’∈PR（S），则 COI（O’）≠COI（O）

（3）O 是无害客体。

中国墙模型也是一种 LBAC 模型。

3．RBAC 模型

与前述模型不同，基于角色的访问控制（RBAC）模型，是一种安全策略的实施方法，基于 RBAC 模型，可以实现自主访问控制，也可以实现多种强制访问控制机制。RBAC 模型通过角色概念来表达访问控制策略的语义结构，角色对应于组织中某一特定职能岗位，代表特定的任务范畴。用户和权限之间通过角色间接发生联系，实现了用户与权限的逻辑分离。这种方式更便于授权管理，角色划分以及职责分担。

RBAC 的理论模型于 1993 年提出；1996 年，Sandhu 提出了被普遍接受的 RBAC 理论模型；2004 年，NIST 提出了 RBAC 的标准，该标准从功能上对 RBAC 进行了四个级别的划分：扁平的（flat）、多级的（hierarchical）、限制的（constrained）以及对称的（symmetric）。

RBAC 提供了一个非常有用的抽象层次，以便于在企业级别而非个别用户级别去提升安全管理。它是一个已被证实可用于大规模授权控制应用的技术。

4.1.5　安全策略模型面临的挑战

安全模型在信息安全的理论研究和工程开发中起到了非常重要的作用，但是，在复杂的实际安全需求面前，安全模型仍有很多局限之处。Zdancewic 于 2004 年提出了信息流安全策略面临的三项挑战。由于大多数安全策略模型都是信息流模型，因此我们也可以把它视为安全策略模型普遍面临的挑战。

Zdancewic 提出的三项挑战分别为：

信息流安全理论和现有体系结构的融合问题。当前的操作系统和软件库并不是按照信息流策略设计的，而基于支持信息流控制的语言来重写所有这些代码显然是不现实的工作。

信息流模型需要避免绝对的无干扰限制，许多应用中，合适的安全策略允许存储秘密信息的实体到普通观察者之间的信息流，而信息流技巧将阻止这些信息流。因此，一个过于严格的信息流分析将禁止一些符合安全需求的程序的执行。

信息流模型需要能够解释和管理复杂的安全策略。一个实际的策略往往不能用简单的无干扰形式的模型来解释，而实际系统还存在与现存的安全体系结构，如由操作系统提供的访问控制机制进行交互的需求，这都需要信息流模型能够对复杂的安全策略有表示和管理能力。

4.2 安全操作系统

我们日常见到的一般是防火墙、防病毒、入侵检测等安全产品，其实，安全操作系统在信息安全中，具有非常重要的地位。安全操作系统在六十年代已经出现，其出现时间远远早于防火墙等安全产品。在国外，安全操作系统始终是科学研究和产品开发的重要方向，国外军方有大量的安全操作系统产品，但由于技术封锁等原因，国内得到的相关信息很少。

安全操作系统最终的目标也是保障其上应用的安全乃至最终信息系统的安全，但它的安全思路，则是从加强操作系统自身的安全功能和安全保障出发，对应用采用“量体裁衣”式的保护方法，在操作系统层面实施保护措施，并为应用层的安全提供底层服务。由于安全操作系统对操作流程和使用方式的约束较大，它主要针对生产型信息系统，即系统流程比较固定、安全需求明确、应用软件来源清晰的系统。针对这类系统，安全操作系统相比较后验式的安全保护方法，具有明显的优势。

安全操作系统是在操作系统层面实施保护措施，这些保护措施主要是对应用访问一些保护措施也可以在应用层实施。那么，如果直接在应用层实施这些保护措施，不是更直接吗？

答案并非如此简单。操作系统的功能是管理信息系统内的资源，应用软件则通过操作系统提供的界面——系统调用接口来访问资源。应用层提供的保护措施可以防止从本应用中发起的非法资源访问行为，但并不能控制通过其它程序发起的攻击行为。如果攻击者通过使用应用外的工具软件、编程攻击等手段发起攻击，应用软件中的安全机制就将被旁路而无法起到保护作用。而操作系统中的安全机制则对所有应用都可以生效，因此难以被攻击者从应用层旁路。同时，它还可以为特定应用提供资源封装和自身保护，限制其它应用访问某应用特定的资源，防止攻击者篡改应用程序，确保应用保护措施的有效性。因此，应用的保护措施，不但不能代替操作系统的安全保护机制，而且需要操作系统的安全保护机制作为它正确实施的基石。

4.2.1 安全操作系统基本概念

对于安全操作系统，并没有一个统一的定义，但访问控制机制是安全操作系统的核心内容，则是安全操作系统领域专家的共识。

安全策略在安全操作系统设计中具有重要地位，它是操作系统一系列安全需求的规范性说明。一般地，我们从保密性，完整性和可用性三个方面来考虑操作系统的安全需求。

保密性一般要求敏感信息仅允许部分有相应授权的人访问该信息，而禁止他人访问。有时，保密性的要求会更进一步，禁止非授权者了解信息的属性，如信息修改时间，信息长度，信息属主，甚至信息是否存在。

完整性指的是数据或资源的可信度，通常使用防止非法的或者未经授权的数据改变来表达完整性。完整性机制可以分为两大类：预防机制和检测机制。预防机制阻止任何未经授权的改写数据企图，或者阻止任何使用未经授权的方法来改写数据的企图。检测机制并不阻止完整性的破坏，它检查出完整性的破坏，并向系统报告数据已不再可信。

可用性是指对信息或资源的期望使用能力。可用性不仅仅是一个安全问题，但对一个安全操作系统而言，必须首先支持应用对信息和资源的合理使用，同时，要考虑防止信息或资源合理使用能力遭到人为的、蓄意的破坏。相比于保密性需求和完整性需求，可用性需求最为复杂，最难以描述。

安全策略中的规范性说明为安全操作系统的访问行为提供了一系列准则。根据这些准则，可以判断一个主体对客体的访问是否符合安全策略。如符合，则安全操作系统允许该访问；否则，安全操作系统禁止该访问。这就是安全操作系统的访问控制机制。

访问控制有两种主要类型，自主访问控制和强制访问控制。自主访问控制类型基于用户身份，确认身份的个人用户可以对所属的资源设置访问控制机制来许可或拒绝对客体的访问；强制访问控制类型基于授权，如果系统内的机制可以控制对客体的访问，而个人用户不能改变这种控制，这样的控制称为强制型访问控制。自主访问控制是安全操作系统普遍实现的安全功能，而高安全级别的操作系统，一般都需要有强制型访问控制机制实施保护。

Anderson 于 1972 年提出的引用监视器模型为系统的访问控制提供了一个基础的抽象模型。这一模型成为访问控制机制的基本模型。Gligor 甚至提出：“引用监视器模型将始终是未来的方向”。

引用监视器对所有系统调用所导致的访问控制进行裁决，其功能可以用图 4-2 来表示：

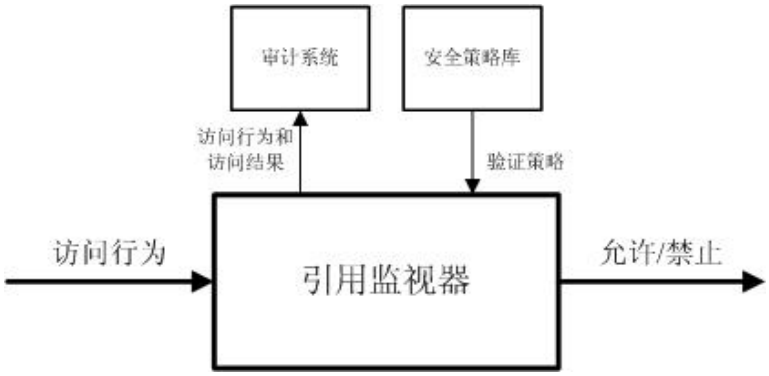


图 4-2　引用监视器原理图

图 4-2 中，引用监视器接收安全策略作为输入，根据安全策略，对访问行为进行裁决，确定该访问行为应当是允许还是禁止，并将访问信息与裁决结果写入审计记录中，发送给审计系统。

一般认为，引用监视器需要一个有效的验证机制，这一机制应当具有以下特征：

1. 该机制应当是独立的，并且具有自我防护或者是防篡改功能。

2. 该机制应当是不可旁路的，应可保证所有主体对客体的访问需要由某些策略来裁决。

3. 该机制应当被设计得足够小，以使其的保护功能可以被充分的分析和测试。

考虑到实际系统的复杂性，Gligor 提出，引用监视器是一个理想化的模型，我们只能用它们去逼近实际中有用的安全策略。而安全操作系统的相关标准中，也只有较高级的系统要求有一个最小化的引用监视器实现，而其它级别的安全操作系统对引用监视器并无形式上的要求。

在一个安全操作系统中，与安全相关的部分的全体被定义为可信计算基，即 TCB。可信计算基是由计算机系统中所有安全保护机制构成的。我国国家标准 GB 17859-1999《计算机信息系统安全保护等级划分准则》定义可信计算基为：计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境并提供一个可信计算系统所要求的附加用户服务。

可信计算基是安全操作系统自身安全性的基石。为了确保安全操作系统自身的安全性，就需要确保 TCB 的设计中遵循一些原则。高安全级别的操作系统要求 TCB 独立于系统的其

它部分，要求 TCB 中不含有和安全无关的内容，并且要求 TCB 的设计具有引用监视器的特性。这些要求其目的是简化 TCB 的复杂度，使 TCB 的安全性可以被比较严格的分析和测试。

4.2.2 安全操作系统发展

从最早的安全操作系统到现在，已经有 40 多年的历史了，安全操作系统开发的指导思想也经历了几次演变，但每一次演变都是在以往安全操作系统知识的继承和发展。回顾这段历史，有助于我们更好地理解安全操作系统概念。

安全操作系统的历史可以从 1967 年 Adept-50 操作系统项目启动之时开始。上世纪六、七十年代，可以看作是安全操作系统的“奠基”时期，在这段时期，安全操作系统的基本思想、理论、技术和方法逐步建立。1969 年，B.W. Lampson 提出了访问控制矩阵模型，1972 年 J.P.Anderson 提出了引用监控机、引用验证机制、安全核和安全建模等重要思想，1973 年，B.W.Lampson 提出了隐通道概念；同年，D.E.Bell 和 L.J.Lapadula 提出的第一个可证明的安全系统的数学模型——Bell&LaPadula 模型。1975 年，J.H. Saltzer 和 M.D. Schroeder 给出了信息保护机制的八条设计原则。1976 年，M.A. Harrison、W.L. Ruzzo 和 J.D. Ullman 提出了操作系统保护（Protection）的第一个基本理论——HRU 理论。1979 年，G.H. Nibaldi 在描述一个基于安全核的计算机安全系统的设计方法时给出了 TCB 的定义。在这段时期，诞生了 Adept-50、Multics、Mitre 安全核、UCLA 数据安全 Unix、KSOS 和 PSOS 等安全操作系统。

在这些研究成果和工程实践的基础上，1983 年，美国国防部颁布了历史上第一个计算机安全评价标准，这就是著名的可信计算机系统评价标准，简称 TCSEC，又称橙皮书。1985 年，美国国防部对 TCSEC 进行了修订。TCSEC 提供了 D、C1、C2、B1、B2、B3 和 A1 共七个等级的可信系统评价标准，每个等级对应有确定的安全特性需求和保障需求，高等级的需求建立在低等级的需求的基础之上。TCSEC 标准针对的是信息系统的安全，但其安全要求可由操作系统很好地实现（操作系统也是一个抽象意义上的信息系统），因而 TCSEC 成为了安全操作系统发展中一个里程碑式的成果，成为了上世纪八十年代多数安全操作系统范型的基础，而它提供的安全等级保护评价准则对后来的信息安全等级保护评价准则，如欧洲的 ITSEC（《IT 安全评估准则》）、六国七方发布的 CC（《通用准则》，后演化成 ISO/IEC 15408 标准），都有较大影响。我国的信息安全保护强制标准 GB 17859-1999 也是以 TCSEC 为蓝本制定的。这一阶段的安全操作系统大多是单一安全策略的操作系统。

随着 90 年代初 Internet 的影响的迅速扩大，分布式应用的迅速普及，单一安全策略的范型与安全策略多种多样的现实世界之间拉开了很大的差距。在这一背景下，美国国防部于 1993 年提出的国防部目标安全体系结构 DGSA 明确提出，国防部的信息系统必须支持多种安全策略下的信息处理，必须支持在拥有不同的安全属性、按照不同的安全保护程度使用资源的用户之间进行信息处理。1997 年完成的 DTOS 项目就实现了对多级安全（MLS）策略、基于标识的访问控制（IBAC）策略和类型裁决（TE：TypeEnforcement）策略等的支持。1999 年诞生的 Flask 系统则在 DTOS 项目的基础上，实现了对多安全策略的动态支持。2001 年发布的 SE-Linux 则将在 Mach 微内核上实现的 Flask 项目移植到了单内核的 Linux 操作系统中，并向开源社区完全公布了源码。

我国也早在上世纪 90 年代就开始了高安全操作系统的研究.。GB 17859-1999《计算机信息系统安全保护等级划分准则》在 TCSEC 的基础上，一定程度上体现出了信息系统的概念，它按照安全性由低到高的顺序，规定了计算机系统安全保护能力的五个等级，一些机构已经实现了满足第三级（安全标记保护级）要求的操作系统，并在满足第四级（结构化保护级）要求的操作系统研究方面也已经取得许多重大进展，其中比较典型的系统包括 SUNIX、COSIXV2.0 安全子系统、LIDS 安全操作系统、SoftOS、安胜操作系统，以及麒麟操作系统等。但由于国内在信息产业方面的相对弱势和资金投入等方面的限制，国内的安全操作系统

在实际应用中还有较大差距。

4.2.3 安全操作系统主要安全技术

本节介绍安全操作系统中主要的安全功能技术和安全保障技术，并说明不同安全保护级别对这些技术的不同要求。

1．身份鉴别

身份鉴别是系统确认实体身份的重要手段。它通过对实体特征信息的检查，确定实体的身份。身份鉴别包括对用户的鉴别和对设备的鉴别。身份鉴别有多种途径，常用的是口令鉴别（包括静态口令鉴别与动态口令鉴别）、安全硬件鉴别和生物特征识别（虹膜、指纹等）。

身份鉴别之前，首先要对用户进行标识。在 GB/T 20271《信息安全技术 信息系统通用安全技术要求》中，根据用户标识和鉴别的不同要求，用户标识的要求分为以下三类：

（1）基本标识：应在可信计算基实施所要求的动作之前，先对提出该动作要求的用户进行标识。

（2）唯一性标识：应确保所标识用户在信息系统生存周期内的唯一性，并将用户标识与安全审计相关联；

（3）标识信息管理：应对用户标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。

其中，基本标识和唯一性标识是操作系统五个级别都要求的，而标识信息管理则是二到五级的共同要求。

用户鉴别则有如下一些具体要求：

（1）基本鉴别：应在可信计算基实施所要求的动作之前，先对提出该动作要求的用户成功地进行鉴别。基本鉴别是五个保护级别的共同要求。

（2）不可伪造鉴别：应检测并防止使用伪造或复制的鉴别信息；一方面，要求可信计算基应检测或防止由任何别的用户伪造的鉴别数据，另一方面，要求可信计算基应检测或防止当前用户从任何其他用户处复制的鉴别数据的使用。这一要求适用于二级以上的保护系统。

（3）一次性使用鉴别：应提供一次性使用鉴别数据的鉴别机制，即可信计算基应防止与已标识过的鉴别机制有关的鉴别数据的重用。这一要求适用于三级以上的保护系统。

（4）多机制鉴别：应提供不同的鉴别机制，用于鉴别特定事件的用户身份，并根据所描述的多种鉴别机制如何提供鉴别的规则，来鉴别任何用户所声称的身份。四级以上的保护系统，都要求至少两种的身份鉴别机制。

（5）重新鉴别：应有能力规定需要重新鉴别用户的事件，即在需要重新鉴别的条件成立时，对用户进行重新鉴别。例如，终端用户操作超时被断开后，重新连接时需要进行重鉴别。四级以上的保护系统，要求重新鉴别的功能。

（6）鉴别信息管理：应对用户鉴别信息进行管理、维护，确保其不被非授权的访问、修改或删除。

四级以上的操作系统要求用户的鉴别信息管理。

对一个已标识和鉴别的用户，应通过用户-主体绑定将该用户与为其服务的主体（如进程）相关联，从而将该用户的身份与该用户的所有可审计行为相关联，以实现用户行为的可查性。

2．标识

标识是强制访问控制的依据。例如，BLP 安全策略模型的实施必须以等级分类和非等级类别组合的敏感标记作为其基础。我们必须为实施强制访问控制的主体和客体指定敏感标记，才可以依据敏感标记，对访问行为进行强制访问控制裁决。系统的标记可以以与主体和客体绑定在一起的方式存在，也可以存放在数据表中，需要使用时，根据主体和客体的特征

字段进行查找。

当数据从安全操作系统安全机制控制范围之内向控制范围之外输出时，根据需要可以保留或不保留数据的敏感标记。根据对标记的不同要求，标记的输出分为：

（1）不带敏感标记的用户数据输出：输出用户数据到安全操作系统安全机制控制范围之外时，不带有与数据相关的敏感标记；

（2）带有敏感标记的用户数据输出：输出用户数据到安全操作系统安全机制控制范围之外时，应带有与数据相关的敏感标记，并确保敏感标记与所输出的数据相关联。

当数据从安全机制控制范围之外向其控制范围之内输入时，应有相应的敏感标记，以便输入的数据能受到保护。根据对标记的不同要求，标记的输入分为：

（1）不带敏感标记的用户数据输入：安全机制应做到，

——在安全机制控制下，从安全机制控制区域之外输入用户数据时，应执行访问控制。

——略去任何与从安全机制控制区域之外输入的数据相关的敏感标记；

——执行附加的输入控制规则，为输入数据设置敏感标记。

（2）带有敏感标记的用户数据输入：安全机制应做到，

——在安全机制控制下，从安全机制控制区域之外输入用户数据时，应执行访问控制。

——安全机制应使用与输入的数据相关的敏感标记；

——安全机制应在敏感标记和接收的用户数据之间提供确切的联系；

——安全机制应确保对输入的用户数据的敏感标记的解释与原敏感标记的解释是一致的。

三级以上的操作系统都需要主体标记、客体标记、不带敏感标记的用户输出、带敏感标记的用户输出，以及不带敏感标记的用户输入。第四级以上的系统则要求实现带有敏感标记的用户输入。

3．审计

审计是事后认定违反安全规则行为的分析技术。在检测违反安全规则方面、准确发现系统发生的时间以及对事件发生的事后分析方面，审计发挥着巨大的作用。这就使得有效的审计子系统成为所有系统关键的安全组成部分。二级以上系统都要求具有审计功能。

审计是基于日志进行的。日志记录系统事件及行为；审计则分析日志记录，并以清晰的、能理解的方式表述系统信息。一个审计系统包含三个部分：日志记录器、分析器和通告器，它们分别用于搜集数据、分析数据及通报结果。

日志记录器响应系统中发生的审计事件，并将审计数据记入审计日志。三级以上系统有实时报警功能的要求，即当检测到有安全侵害事件时，生成实时报警信息，并根据报警开关的设置有选择地报警。四级以上系统则有违例进程终止的要求，要求当检测到有安全侵害事件时，将违例进程终止。五级系统则要求当检测到有安全侵害事件时，取消当前的服务，并将当前的用户账号断开，并使其失效。

分析器对审计数据进行分析，它用一系列规则监控审计事件，并根据这些规则指出事件对系统安全功能的潜在侵害。

三级以上操作系统要求基于异常检测的描述，该描述维护用户所具有的质疑等级——历史使用情况，以表明该用户的现行活动与已建立的使用模式的一致性程度。当用户的质疑等级超过门限条件时，能指出将要发生对安全性的威胁。

四级以上操作系统要求对简单攻击的探测能力，它要求能检测到对系统安全功能的实施有重大威胁的事件的出现。为此，可信计算基应维护指出对安全功能侵害的事件的内部表示，并将检测到的系统行为记录与事件进行比较，当发现两者匹配时，应指出一个攻击即

将到来。

五级以上操作系统要求对复杂攻击的探测，它要求在在四级所要求简单攻击探测的基础上，能检测到多步入侵情况，并根据已知的事件序列模拟出完整的入侵情况，指出发现对安全攻击的潜在侵害的签名事件或事件序列的时间。

安全审计记录应包含客体身份、用户身份、主体身份、主机身份、事件类型等内容。

4．自主访问控制

自主访问控制机制将访问控制的权限交给访问对象的拥有者来自主决定，或者给那些已经被授权控制对象访问的人来决定。拥有者能够决定谁应该拥有对其对象的访问权及内容。自主访问控制是所有级别的安全操作系统都需要具备的安全功能。

根据对自主访问控制的不同要求，自主访问控制的覆盖范围分为子集访问控制和完全访问控制。子集访问控制要求每个确定的自主访问控制，应覆盖由安全操作系统所定义的主体、客体及其之间的操作；完全访问控制则要求每个确定的自主访问控制应覆盖操作系统中所有的主体、客体及其之间的操作。四级以上的操作系统要求完全自主访问控制。

自主访问控制可以有不同的实现粒度。粗粒度的主体为用户组/用户级，客体为文件、数据库表级；中粒度的主体为用户级，客体为文件、数据库表级和/或记录、字段级；细粒度的主体为用户级，客体为文件、数据库表级和/或记录、字段和/或元素级。一级系统要求粗粒度的自主访问控制，二到四级操作系统要求中粒度的自主访问控制，五级操作系统则需要细粒度的自主访问控制。

自主访问控制的实现可以基于主体或者客体来进行。常用的自主访问控制实现方式是基于客体进行的，像 Unix 系统为每个文件提供了一个所属用户、用户组和其它用户对该文件访问权限的标记，Windows 系统则可以维护一个文件自主访问权限的 ACL 表。

5．强制访问控制

强制访问控制通过系统机制控制对客体的访问，个人用户不能改变这种控制。强制访问控制往往基于一些预设的规则来进行，因此偶尔也叫基于规则的访问控制。强制访问控制策略应包括策略控制下的主体、客体，及由策略覆盖的被控制的主体与客体间的操作。可以有多个访问控制安全策略，但它们必须独立命名，且不能相互冲突。

强制访问控制策略一般是根据一个具体的安全模型来实施的，最常用的是用于保密性保护的 BLP 访问控制策略模型，在完整性保护要求比较高的场合，常用 Biba 模型来保障系统的完整性。

与自主访问控制类似，强制访问控制的覆盖范围也可分为子集访问控制和完全访问控制。三级操作系统要求强制访问控制的覆盖范围达到子集访问控制的要求，四级、五级操作系统则要求强制访问控制的覆盖范围达到完全访问控制的要求，更具体地说，四级操作系统要求可信计算基对外部主体能够或直接访问的所有资源（例如：主体、存储客体和输入输出资源）实施强制访问控制。

强制访问控制的粒度分为中粒度和细粒度，中粒度要求主体为用户级，客体为文件、数据库表级和/或记录、字段级；细粒度要求主体为用户级，客体为文件、数据库表级和/或记录、字段和/或元素级。三级、四级操作系统要求中粒度的强制访问控制，五级操作系统则要求细粒度的强制访问控制。

6．客体重用

计算机系统控制着资源分配，当一个资源被释放，操作系统将会允许下一个用户或者程序访问这个资源。但是，已被释放的资源还可能残留着上次使用时的信息，如果一个对某客体没有授权的用户通过资源申请获取了该客体曾经使用过的资源，就有可能获取这些信息。这种攻击被称为客体重用。客体重用可能发生在磁盘、主存、处理器的寄存器和存储器、其它磁介质（例如磁带）或者其它可重用的存储媒体。

为了防止客体重用导致的信息泄露，操作系统在允许下一个用户访问资源之前，需要清除（也就是重写）所有将要重新分配的空间。客体重用攻击对磁介质而言尤为严重，一些精密的仪器可以将最近写入的数据与其先前记录的数据分开，然后再将后者与后者之前的数据分开，依次类推。为防止这类攻击，需要对将要重新分配的空间进行多次重写。另一种解决办法是对磁介质上存储的所有数据进行加密保护，以防止客体重用窃取秘密信息。

二级以上操作系统都需要客体重用保护。

7．可信路径

恶意用户获得不合适访问的一种途径就是“欺骗”用户，使他们认为自己正在和一个合法的安全系统通信，而实际上这时候他们键入的内容以及命令已经被截获且加以分析了。因此，对于关键的操作，如设置口令或者更改访问许可，用户希望能够进行可以信任的通信，以确保他们只向合法的接收者提供这些重要的、受保护的信息。这就是可信路径的需求。

可信路径为用户与可信计算基之间提供一条可信任的通信途径，保护通信数据免遭修改和泄露。利用可信路径的通信可以由可信计算基自身、本地用户或远程用户发起。例如，系统启动时，向用户提供的登录界面应当是由可信计算基发起的；一些操作系统为用户提供了一个唯一的键序列，用户可以通过这个键序列请求一条可信路径；远程用户则可以通过密码机制与本地终端之间建立可信路径。

四级与五级操作系统要求可信路径功能。

8．隐通道分析

隐蔽通道的概念最初是由 Lampson 于 1973 年提出。他在论文《关于限制问题的注释》中这样定义隐蔽通道：“如果一个通道既不是设计用于通信，也不是用于传递信息，则称该通道为隐蔽通道。”

隐蔽通道可以分为时间隐通道和存储隐通道。如果隐蔽通道实现的场景是，一个进程直接或间接地写一个存储单元，另一个进程直接或间接地读该存储单元，则称这种隐蔽通道为隐蔽存储通道。如果隐蔽通道实现的场景是，一个进程通过调节它对系统资源（例如：CPU 时间）的使用，影响另外一个进程观察到的真实响应时间，实现一个进程向另一个进程传递信息，则称这种隐蔽通道为隐蔽定时通道。

四级以上的操作系统要求能够识别系统中的存储隐通道并计算其带宽。

9．形式化分析与验证

形式化方法在高安全级别操作系统的实现中有着重要的地位。四级操作系统要求安全策略的形式化模型，高层设计与低层设计的半形式化说明，五级操作系统则要求高层设计与低层设计的形式化说明。

形式化验证技术分为两大类：归纳验证技术与模型验证技术。一般而言，归纳验证技术在本质上更为通用。归纳验证技术通常需要若干独立步骤来创建公式，以声明系统规范满足属性需求。公式创建完成之后，将被提交给某个定理证明器，定理证明器中使用了诸如谓词演算的高阶逻辑。定理证明器试图通过一系列的证明步骤，从定理的前提开始，最终演化得到定理的结论，从而证明前提和结论是等价的。一些归纳验证技术也用于产品或系统的开发阶段，以便在设计过程中能够找到缺陷。还有一些归纳验证技术用于验证计算机程序的属性。

模型验证技术同样需要确定系统规范与属性集之间的满足关系。模型描述的系统是状态转换系统，同一个公式在某些状态可能是正确的，而在另外一些状态下有可能是错误的。在系统从一个状态转化到另一个状态的时候，公式的真值也可能随之改变。模型检验器验证的属性通常表示为时态逻辑公式。在时态逻辑中，公式的真假是动态变化的，不像在命题逻辑和谓词逻辑中的公式那样真值固定不变。

一般情况下，模型检验器针对单一模型，试图证明系统模型与期望属性的语义等价性，为描述这种等价性，可通过说明模型与属性分别显示出相同的真值表。模型检验方法经常用

于产品开发完成之后、推向市场之前，其检验方法的设计针对于并发系统及那些与环境交互并且永不终止的系统。

形式化验证方法有两个主要困难：

（1）时间：形式化验证方法执行起来很费时间。在每一步给出的断言以及验证断言的逻辑流都是很慢的过程。

（2）复杂性：形式化验证是一个复杂的过程。对某些大的系统没有办法建立和验证断言。对于那些在设计时没有考虑形式化验证方法的系统尤其如此。

在非形式化方法和形式化方法之间，有一个过渡的方法：半形式化方法。半形式化方法有较清晰定义的形式和部分的语义定义，其中的一些基本性质可能通过开发工具进行检查和分析。半形式化方法一般以图、表和结构化英语等方式来表达。

4.3 安全数据库

数据库是电子商务、金融以及 ERP（企业资源计划）系统的基础，通常都存有重要的数据和信息，例如大多数企业、组织以及政府部门的电子数据都保存在各种数据库中。在这些数据中，有很多是敏感甚至涉密的。因此，数据库的安全非常重要。

数据库中数据完整性和合法访问往往会受到很多方面的安全威胁，包括口令策略、系统后门、数据库操作以及本身的安全方案等。但是数据库通常没有像操作系统和网络一样在安全性上受到重视。随着数据库系统的广泛使用和信息系统安全重要性的日趋增长，数据库安全已经不可忽视，其安全已经构成了信息系统安全的基础，显得十分重要。本节介绍数据库系统基本概念、安全风险及对策、安全标准以及安全机制。

4.3.1 数据库系统基本概念

第一个数据库系统是 IBM 公司于 1969 年发布的网状数据管理系统产品 IMS。1979 年，E.F.Codd 提出了关系数据库模型，十多年后，关系数据库以简单灵活、数据独立性高、理论严格等优点表现了强大的生命力。

数据库系统一般可以理解成两部分：一部分是数据库，是指自描述的完整记录的集合。自描述的含义是指它除了包含用户的源数据外，还包含关于它本身结构的描述；数据库的主体是字节流集合（用户数据）以及用以识别字节流的模式（属于元数据，称数据库模式）。另一部分是数据库管理系统（DBMS），为用户及应用程序提供数据访问，并具有对数据库进行管理、维护等多种功能。人们对数据库系统提出的安全要求，实质上是对 DBMS 的安全要求，因为 DBMS 负责执行数据库的安全策略。

一个完善的 DBMS 应具备以下功能：（1）数据库定义，定义数据库结构，包括模式、子模式和存储模式及其映像；定义数据的完整性约束、保密限制等约束条件。（2）数据库操纵，包括数据的初始装入、对数据的访问和更新操作的支持和统一控制，数据库结构的维护与重新组织，数据的存储等。（3）数据控制，包括数据安全性控制、数据完整性控制及在多用户、多任务环境下的并发控制等。

目前最常用的数据库为关系数据库。本节简单介绍关系数据库的一些基本概念。

数据库：由若干个域以及在这些域上所定义的若干关系组成。数据库描述称为关系数据库模式。

关系（表）：对一个关系的描述称为关系模式，包括关系名、属性名、属性向域的映像和属性间数据依赖关系。对应某一关系模式的内容称为相应模式的状态，是元组的集合，简称为关系，可理解为一个二维表。

元组（记录）：对应某一关系中的某一行的内容，是属性值的集合，称为元组或记录。

属性（字段）：关系中每一列的列名称为属性或字段。

为更好地理解数据库系统及其安全问题，有必要了解其体系结构，见图 4-3。

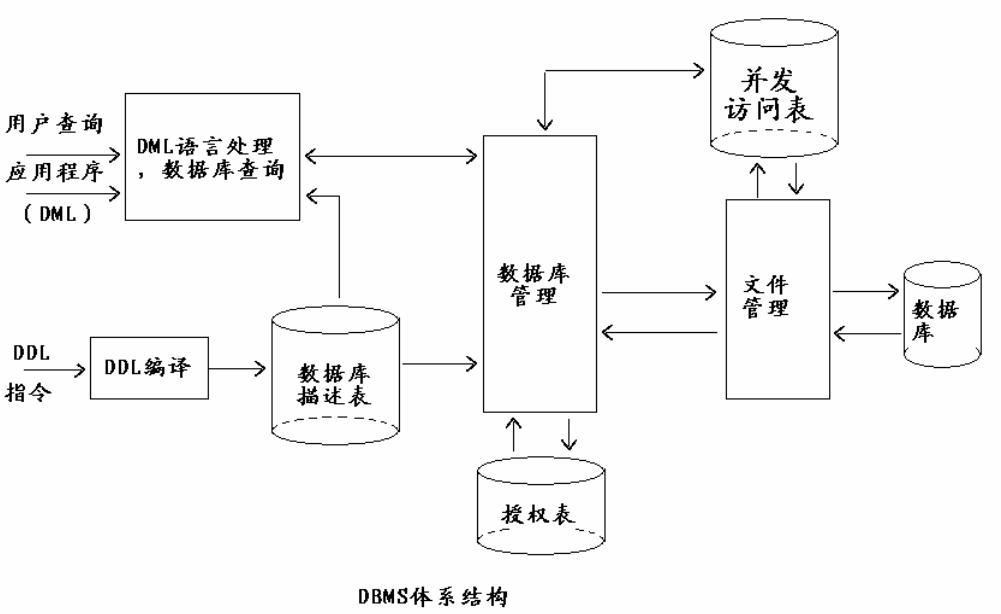


图 4-3　数据库组织结构图

DBMS 为应用程序和用户集中统一管理数据，具体目标为：

- 提供数据共享，集中统一管理数据；
- 减少数据冗余，数据库管理系统集中统一管理数据，使得不同的应用可以共享信息和数据，同时达到减少数据冗余的目的。
- 简化应用程序对数据的访问，通过对 DBMS 的支持，应用程序得以在更为逻辑的层次上访问数据，从而可以简化应用程序对数据的访问。
- 解决数据一致性问题，不同的应用程序在共同的数据环境中运行，同一逻辑数据必须保持一致，才能保证可靠的共享。
- 保证数据独立性问题。数据及数据结构是客观世界的抽象，应用程序则是千变万化的人类活动的要求的体现，DBMS 的主要功能之一是降低程序对数据及数据结构的依赖。

4.3.2　数据库安全威胁

原则上，凡是造成对数据库内存储的数据（包括敏感和非敏感的信息）的非授权访问——读取、增加、删除、修改等，都属于对数据库的数据安全造成了威胁或破坏。另一方面，凡是因业务需要而访问数据库，但授权用户不能正常得到数据库的数据服务时，也称之为对数据库的安全形成了威胁或破坏。

图 4-4 是数据库在网络环境中的位置。由此可知，客户可以通过 web 浏览器和客户端应用程序两种方式连接数据库。严格地讲，该图中任何一个环节上的安全隐患都会对数据库安全造成威胁。

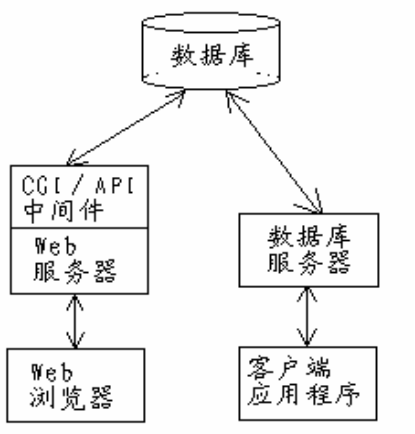


图 4-4　网络数据库结构图

数据库安全的威胁或侵犯大致可以分为以下几类：

- 偶然的、无意的侵犯和/或破坏，自然的或是意外的事故，例如地震、水灾、火灾等导致的硬件损坏，进而导致数据的损坏和丢失。
- 硬件或软件的故障/错误导致的数据丢失，可能导致系统内部的安全机制的失效、非法访问数据的可能、拒绝提供数据服务。
- 人为的失误，操作人员或者系统的直接用户的错误输入、应用系统的不正确的使用，产生与故障相类似的结果。
- 蓄意的侵犯或敌意的攻击，授权用户可能滥用他们的权限。
- 病毒，通常是不可恢复地破坏信息系统，取得信息甚至使对方丧失战斗力。

其它还有诸如泄密、由授权读取的数据通过推理得到本不应访问的数据、对信息的非正常修改、绕过 DBMS 直接对数据进行读写等威胁等。

4.3.3　数据库安全需求

概括地说，数据库安全包括两方面问题，即数据库数据的安全及数据库系统不被非法用户入侵，从而保证数据及信息系统的保密性、完整性、可用性、可追究性等。数据的安全指当数据库数据存储媒体被破坏时以及当数据库用户误操作时，数据库数据信息不至于丢失。数据库系统不被非授权用户入侵指应尽可能地堵住潜在的各种漏洞，防止非授权用户利用它们侵入数据库系统。数据库安全需求体现在以下方面：

（1）完整性，指数据的正确性和相容性。当整个数据库被破坏获某数据项被破坏时，数据的完整性将受到破坏。 数据库的完整性由 DBMS、操作系统和计算机系统管理员保证。包括：

- 物理数据库完整性，即整个数据库的数据不受物理问题的影响，如掉电等，这样在灾难发生后可以重建数据库。
- 逻辑数据库完整性，即数据库的结构是受保护的。例如，一个字段值的改变不能影响其它字段。
- 元素完整性，数据元素的值只能由授权用户改变，即元素的正确性和精确性。

DBMS 通过操作系统保护、两段提交、冗余/内部一致性、恢复、并发控制、监视等手段保证系统完整性。

（2）保密性，保护敏感信息不会直接或间接地被泄漏给未授权的用户。DBMS 在决定是否允许一个访问时，要考虑三个因素：数据的可用性、访问的可接受性、用户的合法性。

通常敏感信息的泄漏包括：

- 数据值，数据值的泄漏是最严重的泄漏；
- 数据值范围，有时值范围也是敏感数据；

- 否定的查询结果，攻击者可精心设计查询方法，从而确定某数据不是某值；
- 信息存在的事实，有时这种事实就是敏感数据，攻击者可精心设计查询方法，从而确定某数据是否存在；
- 可能的取值，有时可以确定某元素具有某值的可能性。

（3）可用性，当系统授权的合法用户申请访问授权数据时，安全系统应保证该访问的可操作性。

（4）可追究性，能跟踪到访问（或修改）数据库元素（数据库、关系、元组）的人。这样的记录可以帮助维护数据库的完整性，至少，在事后可以发现谁在什么时候影响了数据库的什么值。

4.3.4 数据库安全的含义

由于前述威胁的存在，数据库的安全可归纳为保护数据库，以防非授权使用所造成的数据破坏、更改和泄漏。这包含两层含义：系统运行安全和系统信息安全（应用层安全）。

第一层系统运行安全包括：

- 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；
- 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；
- 防止电磁信息泄漏。

第二层系统信息安全包括：

- 用户身份标识和鉴别；
- 用户访问权限控制；
- 数据访问权限、方式控制；
- 审计；
- 数据加密；
- 攻击检测；
- 备份与恢复。

因此，数据库总体安全可由图 4-5 概括。

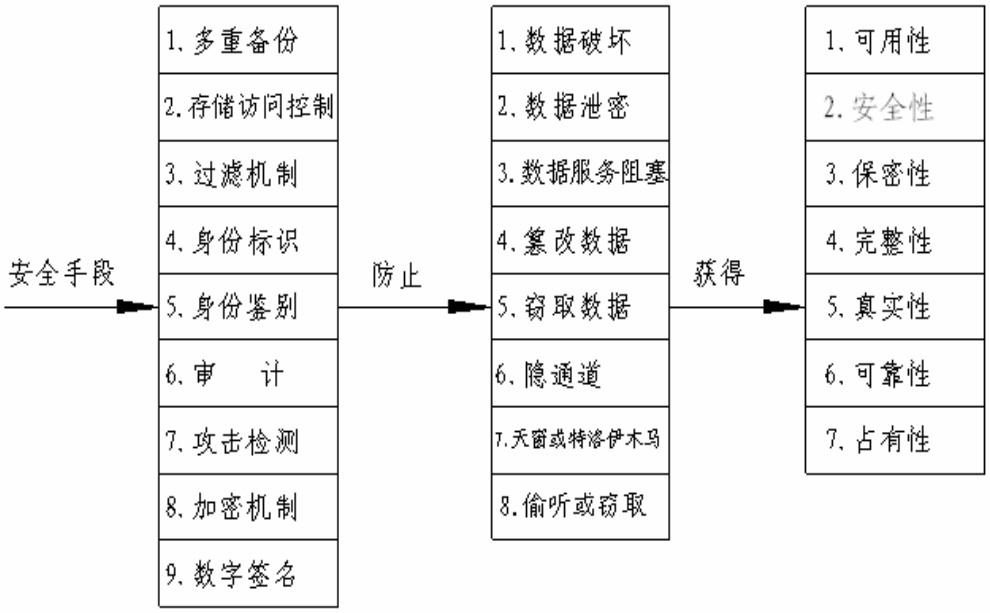


图 4-5　数据库系统的总体保护手段示意图

4.3.4　数据库安全标准与对策

美国国家计算机安全中心（NCSC）颁布了 TCSEC 后，又于 1994 年 4 月继续颁布了《可信计算机系统评估准则的可信数据库管理系统解释》（Trusted Datdabase Management System Interpretation of the Trusted Computer Evaluation Criteria），简称 TDI。它将 TCSEC 扩展到数据库管理系统，是公认权威的数据库安全标准。

TDI 是 TCSEC 向应用软件特别是数据库管理系统扩展的结果，是对 TCSEC 在 DBMS 方面的解释。TDI 在使用中参照 TCSEC，并对 TCSEC 中定义的安全级别、安全目标及各个安全级别的说明都加以继承，同时又对可信计算基 TCB 的概念进一步发展出了 TCB 子集（TCB Subset）。针对不同的 TCB 子集，TDI 将可信 DBMS 上的系统安全策略分割应用于不同的 TCB 子集并根据各个子集要求的异同来分别定义全局要求和局部要求。在 TDI 中也介绍了标准的技术背景、基本概念等以及标准内容。与 TCSEC 的功能相同，TDI 也是为生产者、评估者及研究者提供权威的根据。

目前国内的系统软件和应用软件的安全性级别基本在 C2 级，部分在 C1 级，而 B 级处于开始阶段。在美国的大型 DBMS 中，多数产品已经达到 B1 或相当于 B1 的级别，个别系统已经达到 B2 级。

下面对 TDI 的安全级别划分加以简单说明，它沿用了 TCSEC 的做法，从多个角度来描述每级安全性划分的标准：安全策略、可追究性、保证和文档。

安全策略包括自主访问控制、客体重用、标记（标记完整性、标记信息的扩散、主体敏感度标记、强制访问控制）；可追究性包括标识与鉴别（可信路径）、审计；保证包括操作保证（系统体系结构、系统完整性、隐蔽信道分析、可信设施管理、可信恢复）、生命周期保证（安全测试、设计规范和验证、配置管理、可信分配）；文档（用户指南、可信设施手册、测试文档、设计文档）等。

与操作系统类似，TCSEC/TDI 根据以上指标，将系统划分为四类七个等级，由低到高依次为：D；C（C1，C2）；B（B1，B2，B3）；A（A1）。

4.3.5　数据库主要安全技术

数据库安全可分为三个层次：DBMS 系统层、应用开发层和使用管理层。DBMS 系统层由 DBMS 开发者考虑，为 DBMS 设计各种安全机制和功能；应用开发层由应用系统的开发者根据用户的安全需求和所用 DBMS 系统固有的安全特型，设计相关安全功能；使用管理层要求数据库应用系统的用户在已有安全机制的基础上，发挥人的主观作用，最大限度地利用系统的安全功能。三个层次的基础是安全机制，下面详细介绍这些内容。

数据库的安全策略，通常从系统安全性、数据安全性、用户安全性和数据库管理员安全性等方面考虑。系统安全方面的安全机制可以在整个系统范围内控制对数据库的访问和使用。数据库的安全性与计算机系统的安全性，包括操作系统安全、网络安全是紧密联系、相互支持的。图 4-6 描述了这种关系。

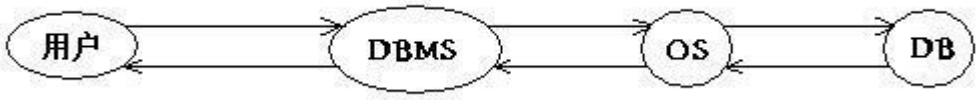


图 4-6　计算机系统安全控制机制关系

数据库常用的安全机制有：

1．身份认证

在开放共享的多用户系统环境下，对于要求进入数据库系统的用户，系统首先根据输入的用户标识进行用户身份验证，只有合法用户才能进入数据库系统。用户身份认证是安全系

统防止非授权用户进入的第一道安全防线，目的是识别系统合法授权用户，防止非授权用户访问数据库系统。用户要登录系统时，必须向系统提供用户标识和鉴别信息，以供安全系统识别认证。标识和鉴别是系统提供的最外层的安全保护措施。目前身份认证最常采用的方法式用户名与口令，即系统为每个合法用户分配唯一的 UserID 和 PassWord。但这种方法可靠性较差，容易被猜出或遭到攻击。因此，该方法对安全强度较高的系统不适用。为此，一些更有效的认证技术得到迅速发展，如智能卡技术、生物特征（指纹、声纹、手图、巩膜等）、数字证书、密码 U 盘等高强度的身份认证技术日益成熟，并取得不少应用成果。

2．访问控制

对于已经进入系统的用户，数据库安全最重要的功能是确保只允许正确的用户访问其权限范围内的数据，这就是访问控制机制的作用。访问控制是安全数据保护的前线，访问控制技术是数据库安全系统的核心技术。访问控制包括定义、控制和检查系统中的主体对客体的访问权限，以确保系统授权的合法用户能够可靠地访问数据库中的数据信息，并同时防止非授权用户的任何访问操作。数据库系统访问控制主要分为：自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC）。大型 DBMS 几乎都支持 DAC。授权涉及用户、对象及该对象上的操作。原则上，只授予用户完成工作必要的权限，即最小权限。MAC 适合于对数据有严格、固定的密级分类的部门。具体实现与操作系统类似，不同的是，数据库的强制访问控制提供更细粒度，如表、元组、属性级的保护。

3．视图机制

同一类权限的用户，对数据库中数据管理和使用的范围有可能是不同的。为此，DBMS 提供了将数据分类的功能，即建立视图。管理员把某用户可查询的数据逻辑上归并起来，简称一个或多个视图，并赋予名称，在把该视图的查询权限授予该用户（也可以授予多个用户）。这种数据分类可以进行得很细，其最小粒度是数据库二维表中一个交叉的元素。通过视图机制可以把要保密的数据对无权访问的用户隐藏起来，从而对数据提供一定程度的保护。该机制提供视图级的安全标识，仅提供用户权限之内的访问数据。

4．存储过程

存储过程相当于在服务器端存储并执行的程序，这些程序组织成函数形式，可以接受参数并返回结果。使用存储过程，然后将存储过程的执行权限授权给特定用户，可以避免用户有过多的不必要的权限。

5。审计

审计将事前检查，变为事后监督机制，通过记录一些用户的活动，发现非授权访问数据的情况。大型 DBMS 提供的审计功能是一个十分重要的安全措施，它用来监视各用户对数据库施加的动作。有两种方式的审计，即用户审计和系统审计。用户审计时，DBMS 的审计系统记下所有对自己表或视图进行访问的企图（包括成功的和不成功的）及每次操作的用户名、时间、操作代码等信息。这些信息一般都被记录在数据字典（系统表）之中，利用这些信息用户可以进行审计分析。系统审计由系统管理员进行，其审计内容主要是系统一级命令以及数据库客体的使用情况。

6。攻击检测

攻击检测是利用日志文件中的数据进行分析，以检测来自相同外部的攻击企图，追查有关责任者，并及时发现和维护系统的安全漏洞，增强相同的安全强度。

7．数据加密

一般而言，数据库系统提供的上述基本安全技术能够满足一般的数据库应用，但对于一些重要部门或敏感领域的应用，仅靠上述这些措施是难以完全保证数据的安全性，某些用户尤其是一些内部用户仍可能非授权获取用户名、口令字，或利用其它方法越权使用数据库，甚至可以直接打开数据库文件来窃取或篡改信息。因此，有必要对数据库中存储的重要数据

进行加密处理，以实现数据存储的安全保护。数据加密是防止数据在存储和传输中失窃的有效手段。数据库的数据加密技术有以下显著特点：（1）加密机制应该是实际上不可破解的；（2）数据加密后的存储空间应该没有明显改变；（3）加密与解密的时间要求更高；（4）灵活的授权机制和加密机制有机的结合；（5）安全、灵活、可靠的密钥管理机制；（6）针对不同加密粒度的处理；（7）加密机制要尽量减少对数据库基本操作的影响。

8．系统安全恢复

随着安全技术的发展，数据库系统要求能对已遭到破坏的系统进行尽可能完整有效的系统恢复，把损失降低到最小程度。

4.4 网络安全

计算机网络（区别于公用电话网和广播电视传输网）是由两台或两台以上的计算机通过网络设备连接起来所组成的一个系统，在这个系统中计算机与计算机之间可以进行数据通信、数据共享及协同完成某些数据处理工作。计算机网络有三大功能：数据通信、资源共享与分布处理。就网络本身而言，其核心的功能是通信。本节从通信安全的角度看待网络安全问题，对于不由网络完成的其它很多安全功能，例如主机安全、边界安全等，则可见于有关信息系统安全的其余知识。

一般而言，网络支持三种不同的数据流：用户数据流、控制数据流和管理数据流。

用户数据流即在网上传输的用户信息。而控制数据流则是为建立用户连接而在网络组件之间传送的各种信息，包括编址、路由信息等。网络基础设施的正确编址是用户通信流的基础，它确保了数据能被传送到目的地址。因此，路由信息的安全性很重要，其作用是保障用户信息能正确传送，并确保用户信息采用的路径不被控制。同样，信令也必须受到保护，以保障用户连接能被正确建立。

管理数据流是网络数据流的第三种类型，是用来配置网络组件或表明网络组件状态的信息，它对于确保网络组件没有被非授权用户改变非常重要。如果网络组件管理遭到破坏，则该组件可能被恶意配置成执行攻击者希望的功能。攻击者只要简单地在网络组件上观察配置信息，就可能会得到网络连接、编址方案或其它可能敏感的信息。与管理数据流有关的网络管理协议包括简单网络管理协议（SNMP）、公共管理信息协议、超文本传输协议（HTTP）、rlogin 和 telnet 命令行接口，或者其它附属的管理协议。

目前，网络技术发展迅速，各类不同的网络所需的信息安全保护也不完全一样。下面重点介绍骨干网的安全，其基本原理也适用于其它网络的安全。

4.4.1 骨干网安全要素

最常用的商业骨干网是 Internet 网。按照骨干网的通用模型，有可以将影响骨干网安全的因素划分为九个主要的方面：网络与网络的通信、设备与设备的通信、设备管理和维护、用户数据接口、远程操作员与 NMC（网络管理中心）的通信、网络管理中心与设备的通信、网络管理中心、制造商交付与维护、制造商环境。如图 4-7 所示。

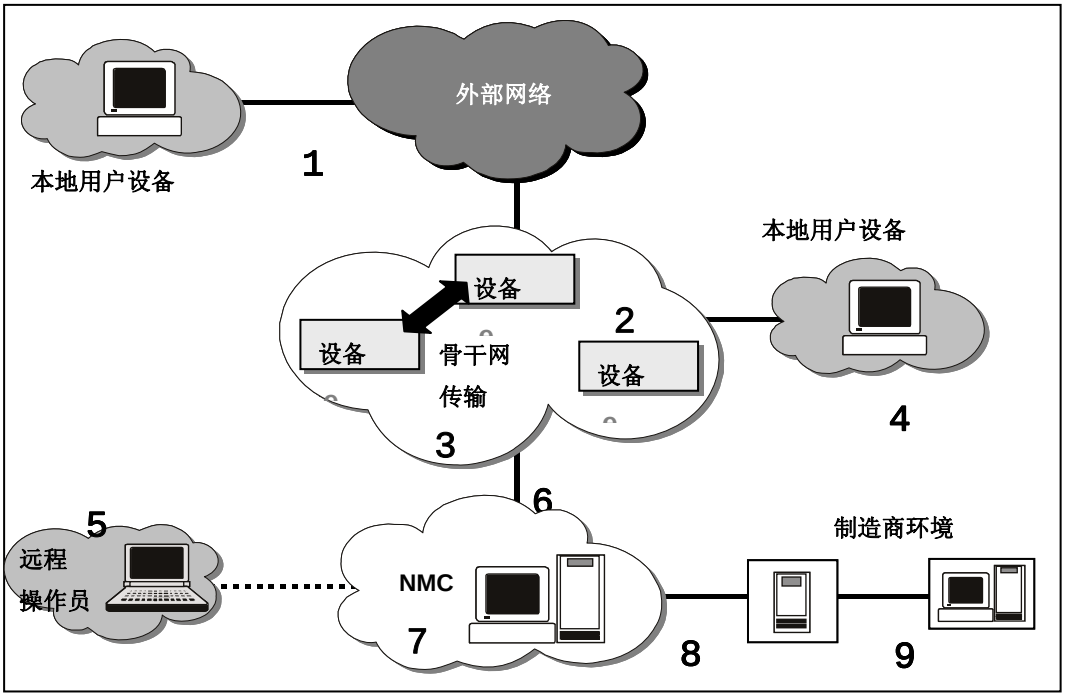


图 4-7　影响骨干网安全的主要方面

以下是对图 4-7 所示的九个安全因素的进一步描述。

网络与网络的通信——这里主要关心两类网络通信数据，一类是传输的用户数据；另一类是控制数据，它用来完成骨干传输设备和外部传输设备之间的通信。一般说来，设备与设备的通信是一个已得到定义良好的协议，它提供面向网络的数据，而这些数据对于传输用户数据很重要。

设备与设备的通信 ——即考虑骨干网内部设备的通信。通常，为了提供最优的性能并支持在线维护，骨干网要求设备之间的管理和控制数据能够无间断地实现信息交换。

设备管理和维护——主要讨论通过配置和参数调整来维护骨干网上的各个设备，以及维护网络管理信息传输。一般说来，每种设备都有自己的一套操作需求和规范，为了使设备不至于在网络上失效，这些操作需求和规范必须由网络管理中心或维护人员控制。

用户数据接口——用户接口是用户数据进入和流出骨干网的通道。用户数据接口可能出现在任何连接处，这些接口应该能够抵抗对用户连接处的进攻。

远程操作员与网络管理中心的通信——主要涉及到操作员的物理安全。例如，这台设备在哪里使用，有什么保护措施等。

NMC 与设备的通信——所有的管理操作都需要 NMC 与组成骨干传输的设备进行互连，因此，需要分析骨干传输以及 NMC 的参数。这种互连可能通过带内或带外信令来实现，并使用主通道或辅助通道。这样就向外提供了访问骨干网设备和网络管理中心设备及其数据的可能性，并使得网络管理数据暴露于外。

网络管理中心——网络管理对于骨干网的可用性来说是相当重要的，故其应该和用户数据分离开来。为了成功地管理好骨干网，需要保护管理设备和数据的安全，以免受到攻击。

制造商的交付与维护——NMC 接收的设备或软件可能用于骨干传输网，且制造商可能被要求直接向骨干传输网设备提供产品服务和维护，即 NMC 可能间接或直接接收来自制造商的信息。因此，确认信息和设备的有效性，防止其被制造商恶意控制，这在骨干网的可用性方面意义重大。

制造商设计与制造——这包括从产品（设备或软件）开发到交付的整个制造过程。安全考虑必须贯穿于整个过程，以便使来自外部的产品能够可信并进行正确操作。

在描述了骨干网安全的几个主要因素之后，有必要继续讨论其通用功能和日常操作。骨干网的特点之一是它有内部和外部的区别。用户通常从骨干网传输部分的外部进行连接，所有内部连接是在骨干传输网的内部或与骨干 NMC 相联。即，NMC 可以认为在骨干网的内部。骨干网的另一个特征是被用户认为它是实现任务目标的途径。用户的需求通常是，他要与另一个实体而不是骨干网本身通信。换言之，用户的信息经过骨干网，但并不保存在骨干网上。

4.4.2 安全要求

可用性是骨干网安全的核心问题。骨干网可用性的基本需求是当需要通过骨干网来完成通信任务时，骨干网能够切实发挥作用。骨干网必须提供充分的响应、服务连续性、通信服务中的抗意外和抗故意中断服务。但是，骨干网不需要提供用户数据的安全服务（例如保密性和数据完整性），这应该是用户自己的责任，而骨干网的核心责任是保证信息不拖延、误传递或不传递。此外，作为端到端的信息传输系统，骨干网提供的服务必须对用户透明。而作为透明需求的一部分，骨干网与其它骨干网或本地网络必须无缝连接。

具体而言，对骨干网的安全要求如下：

1．访问控制

访问控制必须能够区分用户对数据传输的访问和管理员对网络管理与控制的访问。例如，用户对状态信息进行访问时，必须实施比访问配置信息时更强的访问控制措施。

访问控制必须能够限制对网络管理中心的访问。

2．鉴别

网络设备必须能鉴别从其它网络设备处发出的所有通信的来源，例如路由信息。

网络设备必须鉴别网络管理人员的所有的连接要求。

网络管理系统必须在同意访问之前能鉴别网络管理人员。

网络管理中心必须鉴别从外网进入网络管理中心的所有通信源，且必须鉴别制造商提供的材料的来源。此外，网络管理中心还必须鉴别制造商提供的软件的来源。例如，操作系统的新版本在网络上使用之前必须先行鉴别。

在所有拨号用户进入网络管理中心之前，网络管理中心必须对其鉴别。

3．可用性

硬件和软件（例如用户代理和服务器）对用户必须是可用的。服务商必须向用户提供高级别的系统可用性。

4．保密性

网络管理系统必须确保路由信息、信令信息、网络管理通信流的保密性，以保障这些数据的安全。

5．完整性

必须保护网络设备之间通信的完整性。

必须保护网络设备的硬件和软件的完整性。

必须保护网络设备和网络管理中心之间通信的完整性。

必须保护制造商提供的硬件和软件的完整性。

必须保护向网络管理中心的拨号通信的完整性。

6．不可否认性

网络人员不得否认对网络设备的配置所做的改度。此外，制造商不得否认由其提供或开发的软硬件。

4.4.3 安全威胁

网络可用性的威胁可以分为三种：

可用带宽损耗——之所以会出现这种威胁，是因为每一个网络都只有有限的带宽。黑客

的攻击可以减少可用带宽，使合法用户的网络资源受到限制，从而降低网络的可用性。这种攻击通常并不危害网络的操作控制，即网络照常运行，网管中心仍然保持对网络全部资源的管理。可用带宽攻击经常出现在图 4-7 中的 1、2、4 和 6 的组件模型中。

网络管理通信的破坏——这种攻击能威胁网络运行。本质上，网络的功能是通过通信信道将一个用户的信息传给另外的一个用户。这种攻击则通过破坏通信信道，从而威胁到正常的信息传输。例如，攻击者可以割断通信线路或者向网管中心提供错误的路由信息。这些攻击的重点是网络管理信息，以控制信息在网络上的流动。这类攻击常出现在图 4-7 中的 1、2 和 6 中。

网络基础设施失去管理——这种类型的攻击一般是最严重的。它主要表现在使网络基础设备失控。一旦网络管理人员失去对网管中心或网络基础设施的控制，此时的网络资源便有可能被攻击者用来达到其恶意目的。这类攻击经常出现在图 4-7 的 3、7 和 9 中，其结果是导致骨干网控制失灵。

上述每类攻击都表现为使网络的可用性降低。攻击损害的严重程度主要是从网络控制的损失程度来讲的，这是因为对网络的控制意味着网管对攻击的响应能力。

4.4.4 攻击类型

1．被动攻击

被动攻击是监测和收集网络中传输的信息。最初，很多骨干网供应商不把对网络管理数据的被动拦截视为网络面临的威胁，除非攻击者利用收集到的信息发动更危险的主动攻击。例如截获用户账号或口令后以对网络基础设施的控制实施攻击。但目前，骨干网供应商对被动攻击越来越重视，开始逐步意识到网络的拓扑结构是敏感的信息，对它的保护能减少黑客对网络管理通信的攻击。

2．主动攻击

主动攻击是典型的网络外部的攻击。在图 4-7 的骨干网的可用性模型中，外部人员要么是网络用户，要么是通过外部网络进入系统的黑客（区别于作为网络管理员的内部人员）。前面讨论的所有三种威胁都可以通过主动式攻击来实现。

对可用网络带宽的攻击——网络带宽最终决定了网络传输信息的能力。因此，对网络有效带宽的攻击将对合法用户带来重大影响。常见的可用带宽攻击方式有：

- 拒绝服务攻击。这种攻击通过大量假冒的数据包来消耗网络资源，从而“淹没”网络，使网络通信量出现超负荷。由于网络管理系统很难分辨数据包的真假，所以这种攻击很难预防。通常有两种预防的方法，一是给特定的用户优先使用带宽的权利，二是给每个接入点一定的带宽。这种攻击常用在图 4-7 中的 1、2、4 部分。
- 服务的窃取攻击是有效带宽攻击中危害较轻的一种。这种攻击虽然也消耗带宽，但它与正常网络管理操作没有区别。攻击者就像合法用户一样，建立连接，利用网络资源传输信息。大多时候，网络管理人员只有在合法用户收到他们的账单但否认他们使用了这些服务时才能发现这种攻击。典型的预防措施是用户在使用该项业务的时候先要进行鉴别。另外一种预防措施是建立可靠的检测技术，例如系统中事先建立客户的资料，当网络检测到用户的异常活动的时候启动警告信息。这种攻击常出现在图 4-7 模型中的 1 和 4 部分，也出现在 2 和 6 部分中。

网络管理通信的破坏攻击——这种主动攻击可以破坏网络通信，旨在通过攻击网络基础设施设备的控制指令并设法干扰网络中的信息流。与此相反，前述的带宽的可用性攻击不会影响网络的正常操作。它们只是消耗带宽，限制了网络的可用性，但是并不修改网络基础设施设备的指令和操作。这种攻击中，网络管理员仍旧在控制网络，但是网络接收的是会导致服务中断的错误信息。例如，路由器之间传递的网络拓扑信息如果被修改，路由器将无法正常传递用户信息，使网络可用性大大降低。

这种类型的攻击是专门针对骨干网的，专门向如何建立和维护通信路径下手。例如，语音网络利用 SS7 信道管理语音线路，对这种网络的攻击可以是插入一个用户挂断话机的信号，从而导致传输停止。这个领域的攻击要考虑图 4-7 中的 1、2、4、5 和 6 部分。

预防网络管理通信的破坏攻击常用的有两种方法。第一，所有的网络管理信息流都产生于本网络之内，这就需要对进入网络的通信信息进行监测以确保没有网络管理命令从外部进入，这种防御措施关键是建立一个安全的接口。第二，对通信的完整性和权限进行鉴别，例如数字签名可以用于网络通信管理。这种机制能通过把时间戳和序列号嵌入通令流之中来防止信息流的重放攻击。

使网络基础设施失控的攻击——最严重的网络攻击是使网络基础设施操作控制失灵的攻击。对网络基础设施控制发动的攻击可以有以下三种：

- 针对网络操作员和设备之间通信的攻击——这种攻击的目的是切断网络操作员与网络设备之间的联系。例如，网络操作员可能需要通过单一的接入点访问网络，如果接入点遭到攻击将使操作员无法访问网络。这种攻击的最好对策是提供尽量多的接入点，允许网络管理员与网络基础设备之间的自由通信，该对策对后面的攻击方式也有效。
- 直接针对网络设备的网络控制攻击——这种攻击主要是先登录到设备之上，然后对设备进行控制。例如，大部分的网管人员都是通过 Telnet 和其它的网络通信协议远程登录到设备上进行管理。一旦网络操作员有了系统访问权限，便可能改变设备的配置，如改变设备的登录口令。攻击者有很多方法来实现这种攻击，例如攻击者可以通过口令嗅探工具来攻击访问控制机制。对此类攻击有两种可行的对策：在进入网络系统之前进行严格鉴别或者在网络操作员和设备之间建立一条受保护的通道，例如加密的虚拟专用网络。
- 针对网管中心的攻击——如果 NMC 无法操作，网络操作员将完全无法访问网络，也就失去了对网络设备的控制权。每条能够访问网管中心的通道都是潜在的攻击路径。病毒便是网管中心面临的一种威胁。有多种对策来保护网管中心免遭攻击。防火墙可以用来监测进入网管中心的通信，以防止非法通信的访问，阻止病毒的侵入和防范其它的网络威胁。另外一种对策是加强信息安全管理，包括建立 NMC 的灾备中心。

3．内部人员攻击

内部人员指有意或无意造成骨干网可用性降低的用户或网管操作员。在骨干网中，有两种内部人员的攻击，一种是通过远程通信控制骨干网网管中心的操作员，另外是网络组件的开发者和程序员。骨干网中常见的内部人员攻击有：

骨干网网管中心内部人员能够直接访问网管中心资源，他们有权访问和修改网络资源。因此，这些人可以对网络资源控制信息进行恶意的修改。最有效的对策是建立策略机制和严格的访问控制机制。策略机制能把网络访问权限分为关键网络功能，诸如配置，维护和资源提供，以及非关键功能，如电子邮件和网页的访问。此外，可以使用审计机制来检查网络操作的执行过程。

远程操作人员是一种特殊的网络内部人员。这些操作者往往是维护网络的技术专家，但也像其它内部人员一样，是潜在的网络攻击者。有很多网络安全系统缺乏对这类人员的鉴别机制，而他们的操作命令很有可能是不安全的。对此类安全问题的常用的解决方案是加强鉴别机制，对任何远程连接，必须鉴别远程用户的权限，且传输数据的完整性必须得到保护。关于此类攻击，可以参考图 4-7 中第 5 部分。

软件供应商和开发商可以控制很大一部分通信设备，也是一类危险的内部人员，这也是近年来外包服务安全得到高度重视的原因。一些商业软件在开发时缺乏可信软件开发控制机

制，或者某些开发商本身便存有恶意，软件中很有可能嵌入恶意攻击代码。除此之外，为了开发的便利，一些开发商会在软件中后门。如果这些后门在软件应用之后没有及时除去，这些开发人员便有能力攻击网络系统。

对这种内部人员攻击的最有效的对策是在流程上下功夫，包括强有力的软件生产过程流程化管理，包括标明每个模块的需求以及检测方法，并实施强有力的系统配置管理。图 4-7 中的第 9 部分显示了这种攻击。

4．分发攻击

分发攻击是改变供应商提供的软件和硬件，从而实现攻击网络的目的。这类攻击的目标并不局限于开发人员，而且还发生在软件和硬件从开发商到网管中心的安装分配过程中。分发威胁需要考虑到新软件从开发商到安装至骨干网网管中心时的变化过程。有效的对策是利用数字签名技术，使网络管理人员能够鉴别被交付软件的完整性和真实性。分发攻击在图 4-7 中的第 8 部分中表示。

4.4.5 安全措施

网络管理通信的保护——虽然网络管理通信流的内容有时并不敏感，但其完整性和真实性却至关重要。为此，可以使用数字签名技术，且其使用范围应该涵盖所有的关键网络管理通信流。如果还关注网络管理通信流的信息泄露问题，则应该提供保密性机制。

网络管理数据的分离——骨干网的可用性不是依赖于用户数据的保护，而是依赖于网络管理通信流的保护。因此，应该采取措施来分离网络管理通信流和用户数据。一种措施是带外的或专用的通信信道。这样做的意义是使得网络基础设施对用户数据提供保护的同时只对网络性能造成最小的影响。

网络管理中心的保护——网络管理中心是维护网络控制的重要组件。网络管理中心可以利用适当的流程、物理控制或网络安全设备进行保护，目前通用的安全设备是防火墙。此外，网络管理中心还应该约束对网络管理的操作，严格限制操作权限，加强对操作过程的审计。

配置管理——系统管理人员应该加强配置管理操作，以此避免不当的网络配置威胁到网络的安全，并便于网络管理人员在受到攻击之后能快速有效地恢复网络操作。配置管理还应支持新版本网络软件的正确实现和安全系统的升级，并支持严格的安全设计和系统分析。

本章小结

本章介绍了信息系统安全的基础知识，主要由以下内容组成：

（1）信息系统安全模型

BLP 安全模型是历史上第一个有数学基础的访问控制模型，也是最著名的安全策略模型。BLP 安全模型中结合了强制型访问控制和自主型访问控制，该模型影响了许多其它模型的发展，甚至很大程度上影响了计算机安全技术的发展。Biba 模型是一个针对完整性安全需求的模型。简单地将 BLP 模型和 Biba 模型结合在一起，将导致系统中的信息只能在单一的安全等级之间流动，最终使系统无法使用。在 BLP 模型和 Biba 模型结合方面，人们进行了大量的研究工作。本章介绍了一种二维安全策略模型，可以有效应用到实际的信息系统之中。

（2）安全操作系统

操作系统安全是信息系统安全的基础。安全操作系统是指安全级别达到 TCSEC 中 B1 级安全要求的操作系统，其核心的特征是强制访问控制。可信计算基（TCB）是安全操作系统的重要概念，这个概念同样也可以延伸到信息系统之中。它是系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体，是安全操作系统自身安全性的基石。高安全级别的操作系统要求 TCB 独立于系统的其它部分，要求 TCB 中不含有和安全无关的内容，并且要求 TCB 的设计遵循结构化和模块化的准则。这些要求其目的是简化 TCB 的复杂

度，使 TCB 的安全性可以被比较严格的分析和测试。

安全操作系统的主要安全机制有身份鉴别、标识、审计、自主访问控制、强制访问控制、客体重用、可信路径、隐通道分析、形式化分析与验证等。

（3）安全数据库

随着数据库系统的广泛使用和信息系统安全重要性的日趋增长，数据库安全显得十分重要。数据库的安全可归纳为保护数据库，以防非授权使用所造成的数据破坏、更改和泄漏。这包含两层含义：系统运行安全和系统信息安全（应用层安全）。

安全数据库的主要安全机制有身份认证、访问控制、视图机制、存储过程、审计、攻击检测、数据加密、系统安全恢复。

（4）网络安全

网络中有三种不同的数据流：用户数据流、控制数据流和管理数据流。本章重点介绍了骨干网的安全问题。按照骨干网的通用模型，有可以将影响骨干网安全的因素划分为九个主要的方面：网络与网络的通信、设备与设备的通信、设备管理和维护、用户数据接口、远程操作员与 NMC（网络管理中心）的通信、网络管理中心与设备的通信、网络管理中心、制造商交付与维护、制造商环境。骨干网受到的威胁一般有三种：可用带宽损耗、网络管理通信的破坏、网络基础设施失去管理。

骨干网的安全措施涉及到以下方面：网络管理通信的保护、网络管理数据的分离、网络管理中心的保护、配置管理。

习题

1．概述 BLP 模型的主要内容。
2．BLP 模型中，安全标识为什么是非等级类别与等级分类的组合？
3．概述 Biba 模型的主要内容，并阐述 BLP 模型与 Biba 模型的区别。
4．Zdancewic 提出的安全策略模型面临的主要挑战是什么？
5．为什么说安全操作系统是信息安全的基础？
6．什么是可信计算基？
7．安全操作系统主要有哪些安全技术？
8．自主访问控制与强制访问控制的区别是什么？
9．概述客体重用于可信路径的概念。
10．数据库安全威胁包括哪些方面？其安全需求有哪些？
11．安全数据库主要使用了哪些安全技术？
12．骨干网的安全模型中，主要涉及到哪些方面的因素？
13．如何认识骨干网中用户数据的安全问题？
14．骨干网的安全要求有哪些？
15．骨干网主要面临哪些安全威胁？
16．对骨干网的攻击有哪些方式？安全措施是什么？

第 5 章　可信计算技术

本章要点

- 可信计算 TCG 规范
- 可信计算平台密码方案
- 可信平台控制模块
- 可信基础支撑软件
- 可信网络连接

5.1　可信计算概述

“可信”的概念广泛存在于社会生活之中，在不同的场合往往有不同的理解。本节首先给出了在信息技术不同研究领域人们对于可信计算的定义，随后介绍了国内外可信计算的发展及现状，最后针对 TCG 可信计算的概念及其密码技术进行了重点阐述。

5.1.1　可信计算的概念

目前，关于可信尚未形成统一的定义，主要的说法有以下几种。

在容错计算领域，认为可信是指计算机系统所提供的服务是可以论证其是可信赖的。即从用户角度看，计算机系统所提供的服务是可信赖的，而且这种可信赖可得到论证。这个概念不但强调了计算系统的可靠性、可用性和可维性，而且还强调可信的可论证性。

可信计算组织（TCG，Trusted Computing Group）在 1999 年提出可信计算的概念时，对“可信”的定义是：“一个实体在实现给定目标时，若其行为总是如同预期，则该实体是可信的”（An entity can be trusted if it always behaves in the expected manner for the intended purpose），这个概念强调了实体行为的可信。

ISO/IEC 15408《信息技术 安全技术 信息技术安全评估准则》定义可信为：参与计算的组件、操作或过程在任意的条件下是可预测的，并能够抵御病毒和物理干扰。

美国微软公司则在 2002 年提出了可信赖计算的概念，认为可信计算是一种可以随时获得的可靠安全的计算，使人类信任计算机，就像使用电力系统、电话那样自由和安全。

5.1.2　可信计算的发展与现状

1．国际发展

可信计算技术的发展要从容错计算说起。容错计算的研究与发展则应该以1971年召开第一届国际容错计算会议（FTCS-1）为起点。“容错”不是指“容易错”，而是指“容许错”，更确切些说应该是“容许故障”。人们认识到，不论怎样精心设计，选择多么好的元件，物理缺陷和设计错误总是不可避免的，所以需要各种容错技术来维持系统的正常运行。从1975年开始，商业化的容错机推向市场。到九十年代，软件容错的问题被提了出来。进而发展到网络容错。

1983年，美国国防部制定了《可信计算机系统评估准则》（TCSEC），首次提出可信计算基（TCB）的概念，它利用包含最小可信组件集合的可信计算基控制信息流动，从而实现整个系统的可信。随后又推出了被称为彩虹系列信息系统安全指导文件的补充文件。彩虹系列指导文件的出现形成了可信计算的一次高潮。

1996年，IBM Watson实验室开发的安全协处理器IBM 4758充分吸取已有研究成果，是

一个能满足商业需求的高端密码加速器。该协处理器硬件体系包括一个486级CPU，模指数运算加速器，DES、SHA-1运算器，随机数发生器等。协处理器的软件体系包括Miniboot、操作系统和应用三个层次。由Miniboot层负责系统的安全管理和配置；操作系统层负责管理计算、存储及密码相关资源；而应用层则使用操作系统所提供的各项服务。IBM 4758具有认证自身和其软件配置的能力，也允许外部实体认证平台的可信性。

1996年，Bill Arbaugh实现了具有自动恢复功能的安全引导系统AEGIS，并对该过程进行形式化分析。AEGIS以IBM PC平台为原型，修改了标准的引导过程，在BIOS代码中包含了验证代码和公钥证书。它把整个启动过程依次分为四个阶段：阶段0，阶段1，阶段2和阶段3。在计算机加电自检后，进入阶段0，阶段0包含一个小的可信软件集、数字签名、公钥证书以及恢复代码，阶段0是被定义为绝对信任的，自身具有简单的校验和检测。阶段1包含BIOS其余部分的代码，阶段2为扩展卡及其ROM，阶段3为操作系统引导块，阶段4为操作系统。前一阶段验证后一阶段完整性后，运行后一阶段代码。AEGIS引导过程可以选择启动操作系统，或选择启动恢复进程、并修复完整性校验有错误的模块。

九十年代安全协处理器和安全启动的研究为当代可信计算思想的产生奠定了基础。1999年 10 月，Intel、微软、IBM、HP 和 Compaq 共同发起成立了 TCPA（Trusted Computing Platform Alliance，可信计算平台联盟），标志着可信计算进入产业界。TCPA 定义了具有安全存储和加密功能的 TPM（Trusted Platform Module，可信平台模块），并于 2001 年 1 月 30 日发布了基于硬件安全子系统的可信计算平台规范 1.0 版标准。该标准通过在计算机系统中嵌入一个可抵制篡改的独立计算引擎，使非法用户无法对其内部的数据进行更改，从而确保了身份认证和数据加密的安全性。

2003 年 TCPA 改组为可信计算组织 TCG（Trusted Computing Group，可信计算组），标志着可信计算技术和应用领域的扩大。TCG 提出可信计算机平台的概念，并把这一概念具体化到 PC 机、服务器、PDA 和手机和网络连接，提出了可信计算平台的体系结构和技术路线，并推出了以可信平台模块 TPM 为基础的一系列规范，内容包括可信平台模块、软件栈、主机、网络连接等，这些规范描述了以 TPM 为核心的可信计算平台体系结构。

TCG 提出的可信平台体系结构将一个具有密码运算功能的专用密码芯片 TPM 嵌入到计算机主板，通过一系列密码技术和信任链技术，实现计算平台的完整性、身份可信性和安全存储等功能，增加了计算平台的安全性。这种结构除了信息的保密性，更强调了信息的真实性和完整性。但在工程实践中，发现这种结构存在一些问题，比如可信根构成、信任链建立、可信网络接入认证等。

2003 年，Intel 正式推出了支持 Palladium 的 LaGrande 技术，用于保护敏感信息的硬件架构，简称 LT 技术。其核心是在原来硬件基础上增加一层可信机制，其目的是保护 PC 可能遭受的基于软件，甚至基于硬件的攻击。LT 是一组强化的硬件部件，包括微处理器、芯片组、I/O 设备及其相应软件。

同年，微软将 Palladium 改名为 NGSCB（Next-Generation Secure Computing Base，下一代安全计算基）。2005 年，微软将“瘦身”版的 NGSCB 嵌入到新一代操作系统 Vista 中，其中包括安全启动和数据存储保护等功能。而 NGSCB 的目的是为构建下一代安全计算平台环境提供基于软硬件的整套方案。

2006年，IBM的Reiner Sailer和Trent Jaeger等人为Xen虚拟机设计实现了“虚拟TPM”，一个可信计算硬件同时能够为多个运行的操作系统提供安全服务。为此，他们扩展了现有TPM规范的指令集，使多个用户能透明地使用一个TPM，并大大提高了可信计算硬件的使用效率。

2007 年，Intel 正式发布了可信执行技术（Trusted Extension Technology，简称 TXT）。该技术主要是通过硬件内核和子系统来控制被访问的计算机资源。该技术可以应付计算机病

毒、恶意代码、间谍软件和其它安全威胁。TXT 技术具备以下保护功能：处理器执行内存、处理器事件处理、系统内存、内存和芯片组路径、存储子系统、人为输入设备和显卡输出等。

2．国内发展

相比于国外可信计算的发展，我国在可信计算技术研究方面起步较早，技术水平不低。在可信芯片、可信计算机、安全操作系统、可信计算标准制定等方面都先后开展了大量的研究工作，并取得了可喜的成果。

早在 1992 年，我国专家发明了微机保护卡，利用了密码技术解决 DOS 运行环境中的 PC 机安全保护问题，达到了无病毒、自我免疫的效果。其核心技术是采用了二进制可执行代码的加密保护，加载运行时进行完整性校验，不符合合法授权的程序无法运行，病毒自然也无法进来。即使恶意代码或病毒进入系统，也无法破坏关键的应用程序和系统文件，因为关键的可执行代码通过密码机制进行了保密性和完整性保护。在这一思想影响下，国内当时还出现了许多类似的基于硬件的防病毒卡。这可以认为是我国早期对可信计算的研究。

1992 年之后，我国专家进一步在安全操作系统研究中提出和应用了完整性保护思想，结合完整性校验等机制实现了高安全等级操作系统中的代码保护。这些思想体现了密码技术在安全操作系统的保障作用，也是可信计算的实际应用。

2000 年 6 月，武汉瑞达和武汉大学合作，开始研制安全计算机，并且在专家指导下，将平台认证、代码保护、密码校验等机制加入安全计算机方案，其核心思想是采用了可信计算。该成果在 2004 年 10 月通过鉴定，被认为是“国内第一款可信计算机”。

2005 年 4 月，联想集团的 TPM 芯片和可信计算机相继研制成功。同年，兆日公司的 TPM 芯片也研制成功，同方、方正、浪潮、长城等公司也推出了可信计算机样机，加入了可信计算的行列。至此，中国的可信计算产业揭开了序幕。但此后很快发现，国内在技术上盲目跟踪 TCG，我国可信计算产业的发展受到很大局限。

2005 年 12 月，国内组织了知名芯片厂商和从事可信计算产品研发的公司及科研单位，成立了“可信计算密码支撑平台联合工作组”，开始对可信计算密码标准进行预研。2006 年，联合工作组在北京工业大学多次集中攻关，研究编写可信计算平台密码方案，完成了“可信计算密码规范”和“可信计算平台密码规范测评规范”编制任务。这些成果被专家验收意见认为对形成我国可信计算平台密码相关标准和专利奠定了良好基础，为推动我国可信计算产业发展提供了有力的密码技术支撑。

2007 年 2 月，北京工业大学、电子四所、华为、长城、中标软等十三家单位，在“可信计算平台密码”基础上，研究制定“可信平台控制模块规范”等四个面向主机的标准，完成了《可信平台控制模块规范》、《可信平台主板功能接口规范》、《可信基础支撑软件规范》、《可信网络连接架构规范》标准草案，形成了可信计算标准系列的主体框架，解决了芯片、软件栈、主机平台和网络连接基本结构等主要问题。

2007 年 12 月，国家密码管理局发布了《可信计算密码支撑平台功能与接口规范》，该规范以上述“可信计算密码规范”为指导，描述了可信计算密码支撑平台的功能原理与要求，并定义了可信计算密码支撑平台为应用层提供服务的接口规范。可信计算密码规范与标准的制定，为我国可信计算的发展方向和广泛应用起到了基础性的引导和促进作用。

2007 年之后，包括 973、863、国家自然科学基金等科研基金以及信息产业部、发展改革委等部委的产业发展基金，都对可信计算相关技术研究和产品开发进行了大力支持。

2008 年 4 月，为促进我国可信计算技术发展，由企事业、科研单位、相关用户和个人组成的中国可信计算联盟（CCTU）成立，旨在以企业为主体，产学研用联合，促进我国可信计算产业链的形成和发展，增强企业竞争力。

此外，我国对于可信计算在系统中的应用也进行了相应的探索，例如公安部实施的信息系统等级化保护试验平台建设项目中，充分发挥了可信计算在高安全等级信息系统中的保障

作用。

当前，可信计算技术已经过了几十年的发展历程，目前，无论是在国际还是国内都已成为信息安全领域研究的热点和趋势。

5.1.3 可信计算 TCG 规范

可信计算组织在 TCG 规范中确立的可信计算基本思想是，首先构建一个信任根，再建立一条信任链，从信任根开始到硬件平台，到操作系统，再到应用，一级认证一级，一级信任一级，把这种信任扩展到整个计算机系统，从而确保整个计算机系统的可信。从信任根出发，通过信任链进行信任传递，来解决 PC 机结构所引起的安全问题。

可信计算平台的信任根分为三部分，分别为可信度量根（RTM，Root of Trust for Measurement）、可信存储根（RTS，Root of Trust for Storage），以及可信报告根（RTR，Root of Trust for Reporting）。可信度量根是指一个能够进行完整性度量的计算引擎，也是度量计算系统的起始点。可信存储根是指一个能够可靠进行安全存储的计算引擎。可信报告根是指一个能够可靠报告 RTS 所保存信息的计算引擎。

信任链的建立是以从可信度量根为起点，建立的过程包含了完整性的度量和存储。完整性的度量是指任何想要获得平台控制权的实体，在获得控制权之前都要被度量。完整性的存储指对实体完整性的度量值将被可信平台模块 TPM 保存，该过程的度量事件同时存入内存或硬盘日志中。完整性报告是指可信平台模块提供其保护区域中完整性的度量值、日志中的度量事件和相关的证书，质询的一方可以通过完整性报告判断平台的状态。

TCG 可信计算以 TPM 为核心，逐步把可信由 TPM 推向网络和各种应用。TPM 是一个具备多种密码支持部件、安全功能部件和存储部件的小的片上系统。它完成了可信存储根和可信报告根的功能。TPM 主要包括输入/输出（I/O）、非易失性存储器（Non-Volatile Storage）、平台配置寄存器（PCR）、身份认证密钥（AIK）、程序代码（Program Code）、随机数发生器（RNG）、Sha-1 引擎（SHA-1 Engine）、密钥生成器（Key Generation）、RSA 引擎（RSA Engine）、选择进入（Opt-in）和执行引擎（Exec Engine）。

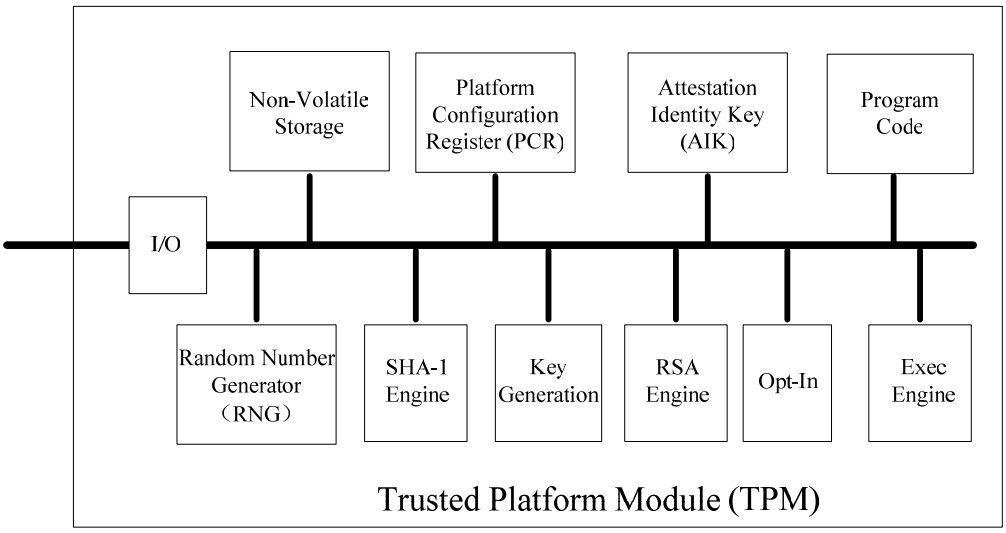


图 5-1　TPM 结构

密码技术是 TPM 实现其安全功能的基础，下面主要从密码算法、密钥管理、授权协议、证书管理等方面分析 TCG 的密码技术。

在密码算法方面，由图 5-1 可以看出，TCG 主要使用了两种算法，使用输出长度为 160 比特的 sha1 算法作为杂凑算法并且用来支持 HMAC 运算，使用密钥长度为 2048 位的 RSA 算法作为非对称密码算法。TCG 并没有明确引用对称密码算法，主要使用非对称算法 RSA。但是对于 RSA 算法，为保障其安全性，一般认为密钥的位数必须在 1024 位以上的字长才有

安全保障。

在密钥管理方面，TCG 的密钥体系，密钥类型繁多，并且管理复杂，包括如下七种：

- 签名密钥（Signing Key）：非对称密钥，用于对应用数据和信息签名。
- 存储密钥（SK-Storage Key）：非对称密钥，用于对数据或其它密钥进行加密。存储根密钥（SRK-Storage Root Key）是存储密钥的一个特例。
- 平台身份认证密钥（AIK-Attestation Identity Key）：专用于对 TPM 产生的数据（如 TPM 功能、PCR 寄存器的值等）进行签名的不可迁移的密钥。
- 签署密钥（EK- Endorsement Key）：平台的不可迁移的解密密钥。在确立平台所有者时，用于解密所有者的授权数据和与产生 AIK 相关的数据。签署密钥从不用作数据加密和签名。
- 绑定密钥（Binding Key）：用于加密小规模数据（如对称密钥），这些数据将在另一个 TPM 平台上进行解密。
- 继承密钥：在 TPM 外部生成，在用于签名和加密的时候输入到 TPM 中，继承密钥是可以迁移的。
- 验证密钥：用于保护引用 TPM 完成的传输会话的对称密钥。

在证书管理方面，定义了五类证书，分别为签署证书（Endorsement Credential）、符合性证书（Conformance Credential）、平台证书（Platform Credential）、认证证书（Validation Credential）和身份认证证书（Identity or AIK Credential）。

5.1.4 可信计算平台体系结构

可信计算平台是构建在计算系统中并用来实现可信计算功能的支撑系统，构造以密码技术为基础，以可信平台控制模块为信任根，可信主板为平台，可信基础支撑软件为核心，可信网络连接为纽带的体系结构。

如图 5-2 所示，可信计算平台由四部分组成，由下到上分别是以密码算法、密码协议和密钥管理等密码技术为基础的可信平台模块，实现信任链建立和维护的可信平台主板，实现信任链向安全应用扩展的可信基础支撑软件以及实现信任由单个主机扩展到多个主机的可信网络连接。

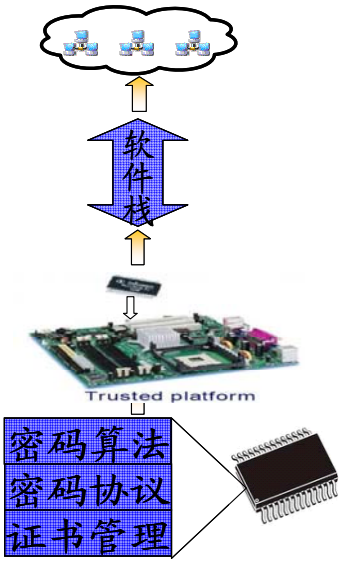


图 5-2 可信计算平台基本框架

可信计算平台实现平台完整性度量与报告、平台身份可信和数据安全保护等安全功能。图 5-3 描述了可信计算平台的三大功能及其体系结构。

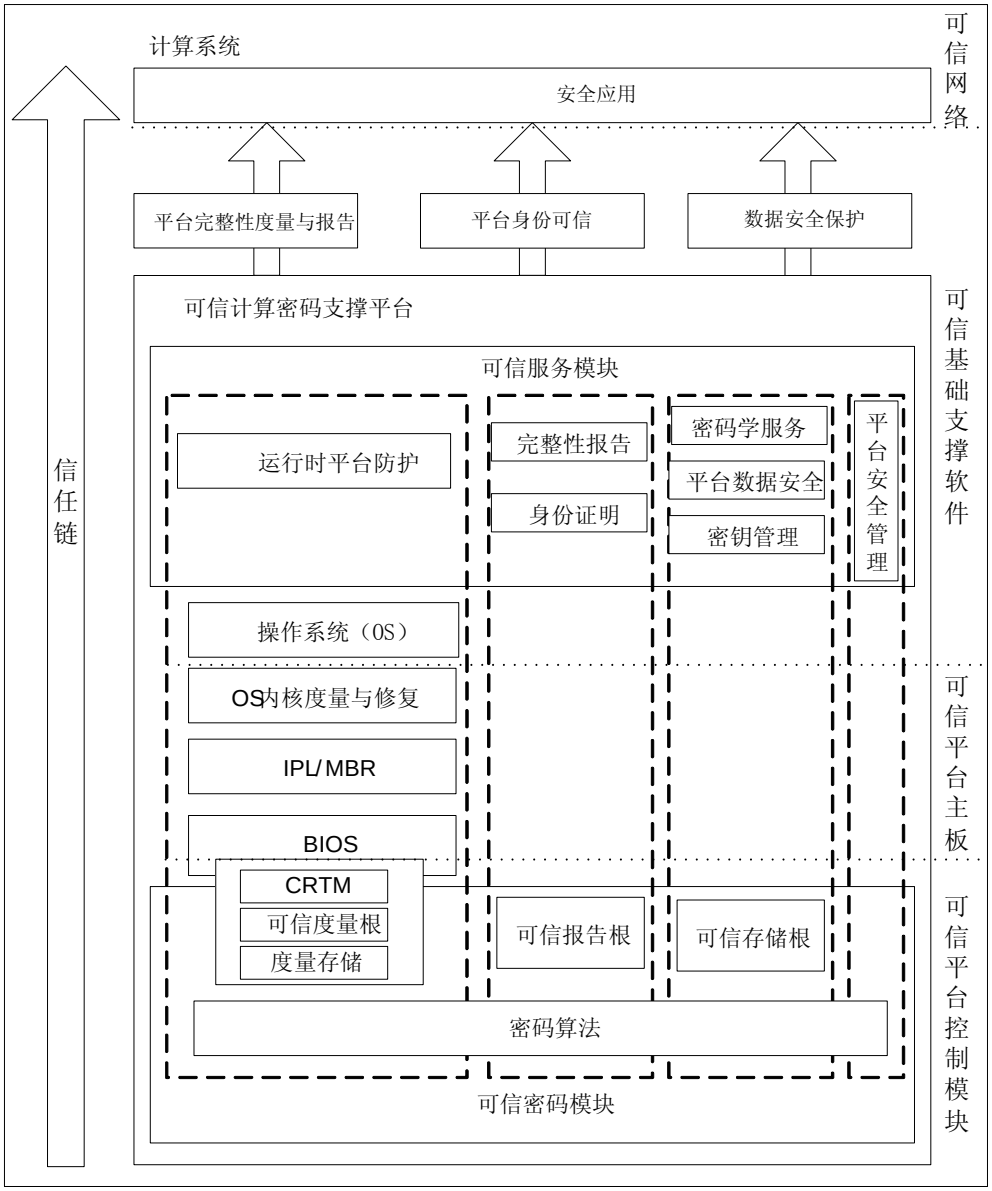


图 5-3　可信计算平台功能和体系结构

下面将分别针对可信计算平台中的密码技术、可信平台控制模块、可信平台主板、可信基础支撑软件以及可信网络连接五个部分进行简要概述。

在密码技术方面，针对 TCG 密码方案中在密码算法、密钥管理、授权协议和证书管理等方面存在的一些问题，设计了与其不同的密码方案，主要表现在密码算法配置、密码使用、密钥管理、证书管理等方面，为平台自身的完整性、身份可信性和数据安全性提供密码支持。密码技术是支撑可信计算平台体系结构的基础。

可信平台控制模块（TPCM）是一种集成在可信计算平台中，用于建立和保障信任源点的硬件核心模块，为可信计算提供完整性度量、安全存储、可信报告以及密码服务等功能。可信平台控制模块作为信任度量的起点包括可信度量根、可信存储根和可信报告根三个信任根。以可信平台控制模块为基础，可以扩展出可信计算平台的可信度量功能、可信报告功能与可信存储功能。可信平台控制模块是可信计算平台体系结构中的信任根。

可信平台主板是以一个完整的、可控子系统方式运行在通用计算机系统中，结合密码技术工具，通过在系统内建立和维护信任链，为通用计算机提供安全可信的运行环境。主要功能是建立基于可信平台控制模块（TPCM）的静态信任链，信任链的建立范围是基于 TPCM

开始，传递到操作系统内核（OS kernel）运行之前。其主要意义在于：开机第一时刻起，实现基于 TPCM 的信任链建立。可信平台主板是可信计算平台体系结构中信任链建立和维护的平台。

可信基础支撑软件是可信计算平台支撑体系中的基础软件部分，能够保障信任链在软件系统的传递，保证系统软件的可信性，为应用开发提供必要的标准编程接口，管理可信计算平台的可信资源。可信基础支撑软件体现了两方面功能。首先，可信基础支撑软件是整个可信计算平台信任链传递中重要的部分，可以与系统安全机制和安全策略相结合，有效保障可信计算基（TCB）在软件部分的扩展。其次，可信基础支撑软件对应用软件提供完整性度量、身份认证和数据保密性等服务，并为应用软件使用这些服务提供了编程接口。可信基础支撑软件是可信计算平台体系结构的核心。

可信网络连接架构在终端接入网络之前对其平台状态进行度量，只有满足网络安全策略的终端才被允许接入网络，使对网络有潜在威胁的终端不能直接接入网络，同时，终端也对接入服务器进行验证，只有满足终端安全策略的接入服务器才允许与终端连接，这是一种主动、双向的、预先防范的网络连接方法。可信网络连接架构是可信计算体系结构的一个重要组成部分，是具有可信平台控制模块的终端与可信网络连接的架构，目的是使信任链从终端扩展到网络，将单个终端的可信状态扩展到互联系统。可信网络连接是可信计算平台之间互联的纽带。

本节针对可信计算平台体系结构的五个方面做了简单的概述，以使读者有一个整体的了解，下面几节将分别针对可信计算平台密码方案、可信平台控制模块、可信平台主板、可信基础支撑软件以及可信网络连接进行详细讲解。

5.2 可信计算平台密码方案

密码技术是可信计算平台的基础，由 5.1.3 可以看出，TCG 的密码技术在密码算法、授权协议存在着问题，并且密钥和证书类型繁多，针对这些不足，我国的“可信计算密码规范”课题设计了与 TCG 不同的密码方案，构成了我国的自主的可信计算标准的基础。该方案使用对称算法与非对称算法相结合的密码算法，精简了授权协议，简化了密钥和证书类型。

本节首先讲述了可信计算平台的主要功能和密码之间的关系，包括平台完整性度量与报告、平台身份可信、平台数据保护三个功能以及 SCH、ECC、SMS4 三个密码算法。然后分别针对可信计算密码方案中的密码算法配置、密码的使用、密钥管理和证书管理等方面进行讲解。

5.2.1 密码与可信计算平台功能的关系

密码技术是可信计算平台的基础，为可信计算平台实现其安全功能提供密码支持。可信计算平台实现如下三大功能：

1．平台完整性度量与报告

利用密码机制，通过对系统平台组件的完整性度量，确保系统平台完整性，并向外部实体可信地报告平台完整性。

2．平台身份可信

利用密码机制，标识系统平台身份，实现系统平台身份管理功能，并向外部实体提供系统平台身份证明和应用身份证明服务。

3．平台数据安全保护

利用密码机制，保护系统平台敏感数据。其中数据安全保护包括平台自身敏感数据的保护和用户敏感数据的保护。另外也可为用户数据保护提供服务接口。

密码与平台功能关系如图 5-4 所示：

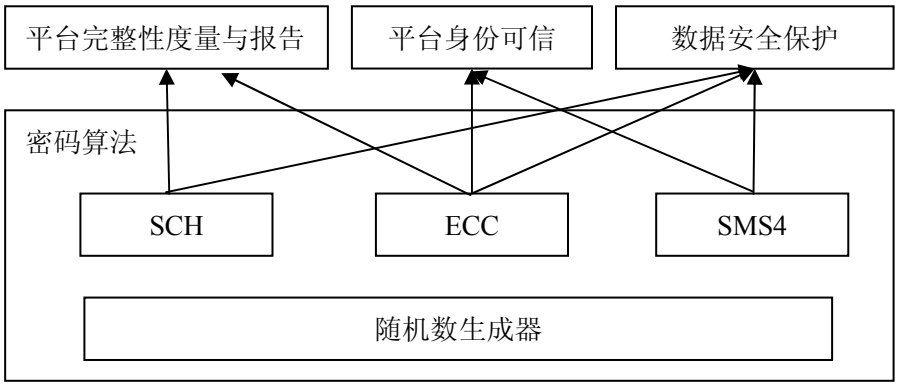


图 5-4　密码与平台功能关系

5.2.2　密码算法配置

可信计算密码支撑平台中配备的密码算法包括：随机数产生算法、杂凑算法、消息验证码算法、对称密码算法和公钥密码算法。

随机数产生算法和模块由各可信计算芯片制造商设计实现，但必须满足国家商用密码随机数检测规范的要求。

杂凑算法为我国自主研制的 SCH 密码算法，杂凑算法分为消息预处理和消息迭代处理，经预处理的消息分组长度为 512 比特，杂凑值长度为 256 比特。

消息验证码算法（HMAC），利用杂凑算法 SCH，对于给定的消息和验证双方共享的私钥产生长度为 t 个字节的消息验证码，消息验证码产生过程采用美国联邦信息处理标准 FIPS 198 中的消息验证码产生过程。

对称密码算法使用我国自主研制的 SMS4 算法，密钥长度 128 比特，明文分组长度 128 比特，密文分组长度 128 比特。

公钥密码算法使用 F_p 上的 ECC 国家标准算法，密钥位长为 m（m=256）。一般利用 RSA 协该算法涵盖系统参数、密钥对产生、签名/验证算法、加密/解密算法和密钥协商共五个方面。

5.2.3　密码使用

1．密钥迁移

为保证平台在发生灾难性的事件时能正常恢复受保护的存储数据和保证应用的正常使用，需要把相应的存储密钥和签名密钥予以迁移备份。迁移需要保证密钥的保密性和完整性，并确保待迁移密钥是可信密码模块里的密钥和目的平台是一个可信计算平台。

假定要将平台 A 的一个可迁移密钥 migratedKey 迁移到平台 B 上，其迁移过程描述如下：

1） 平台 B 将平台加密证书（记为 PEKbCert），发送给平台 A。平台 A 验证 B 的证书，确认平台 B 是一个可信平台。

2） 平台 A 将被迁移的密钥 migratableKey 的密文数据 Enc_migratableKey 加载到 TPCM 中, TPCM 解密出被迁移的密钥 migratableKey；

3） 平台 A 随机产生一个对称加密密钥 SymKey，该密钥将用于加密被迁移的密钥 migratableKey；

4） 使用 SMS4 算法，用 SymKey 加密被迁移的密钥 migratableKey，生成被迁移密钥数据 MigratedData，MigratedData＝SMS4_Encrypt（SymKey，migratableKey）；

5） 用平台 B 的平台加密密钥 PEK 的公钥 pubPEK 加密对称密钥 Symkey，

Enc_SymKey＝ECC_Encrypt(pubPEK, SymKey)；

6） 将迁移数据 MigratedData，已加密的对称加密密钥 Enc_SymKey 从平台 A 传递到平台 B；

7） 平台 B 使用用平台 B 的平台加密密钥 PEK 的私钥 privPEK 解出对称加密密钥 SymKey， SymKey＝ECC_Decrypt(privPEK, Enc_SymKey)；

8） 使用 SMS4 对称算法，用对称加密密钥 SymKey 解密迁移密钥数据 MigratedData，得到被迁移密钥 migratableKey，migratableKey＝SMS4_Decrypt(SymKey，MigratedData)；

9） 平台 B 将被迁移密钥 migratableKey 重新加密，并存入平台 B 的加密保护存储区，从而完成整个迁移过程，New_Enc_migratableKey＝SMS4_Encrypt(Keyb，migratableKey)。

2．授权协议

授权协议（Authorization Protocol）为外部实体与 TCM 之间的访问协议。协议实现了外部实体与 TPCM 之间的授权认证、信息的完整性验证和敏感数据的保密性保护。

在外部实体访问和使用 TPCM 时，首先建立对实体的授权协议，才能利用 TPCM 的功能实现密码算法支持；建立的规则如下：

1） AP 会话以 TPCM_AP_CREATE 命令发起，以 TPCM_AP_TERMINATE 终止。

2） 协议提供认证机制。以 AuthData 为共享秘密生成会话密钥，并基于该会话密钥生成校验值，用以判断调用者是否拥有对某一实体的权限。

3） 协议提供完整性保护机制。以双方共享的会话密钥对功能调用阶段的数据包进行完整性保护。

4） 协议提供抗重播机制。seq 为抗重播序列号，由 TPCM 生成并在外部调用者和 TPCM 之间共享。双方各自维护序列号，每发送一个数据包序列号自增 1，用以防止重播攻击。

5） 建立了外部实体的授权会话后，外部实体可以对 TPCM 进行自己可以进行的操作；例如建立所有者授权会话后可以对 TPCM 管理、启动 TPCM、使 TPCM 有效或无效、清除 TPCM 内部数据、升级 TPCM 内部固件程序、修改所有者授权等等；建立用户密钥授权会话后可以利用该密钥进行数据加解密、签名验证、密钥协商、密钥迁移等操作。

3．DAA 数字签名

DAA 是一个为 TCG 设计的基于零知识证明理论的签名方案：签名者为 TPM，验证者为外部实体，TPM 规范 1.2 版本支持 DAA 协议。

DAA 的含义为：

Direct proof – 不借助可信第三方

Anonymous – 不暴露 TPM 的身份

Attestation – 表明来自某个 TPM

典型的 AIK 证书发布是基于可信第三方的，而 DAA 的目的是在不借助可信第三方，且不暴露 TPM 身份的情况下，使验证者相信 AIK 密钥来自某个合法的 TPM。

DAA 协议的参与者有：发布者（ISSUER）、可信平台模块（TPM）、主机（HOST）、VERIFIER（验证者）。其中 HOST 指包含 TPM 的可信计算平台。

DAA 方案包含两个协议：JOIN 协议和 SIGN 协议。

下面是 DAA 协议的基本描述。

ISSUER 产生密钥对，IKEY 是密钥对的公钥，称为发布密钥。

JOIN 协议是在 ISSUER 和(TPM,HOST)之间进行的，协议完成后，(TPM,HOST)会收到一个 DAA 证书。在协议过程中，TPM 产生一个 DAA 私钥 privDK。TPM 通过 EK 向 ISSURE 证明自己的身份。如果 JOIN 协议成功，ISSURE 会为(TPM, HOST)产生 DAA 证书－certDK。TPM 可以借助 DAA 证书和 DAA 密钥的私钥来产生可以用 IKEY 验证的数字签名。

SIGN 协议是在 VERIFIER 和(TPM, HOST)之间进行的，该协议可以使 VERIFIER 确认

一个 AIK 是来自有效的 TPM。

TPM 产生 AIK，并使用 DAA 密钥私钥对 AIK 公钥签名，TPM 将 AIK 的公钥和对 AIK 公钥的数字签名发送给验证者。验证者使用 IKEY 验证这个数字签名，从而可以判断对应的 AIK 私钥是否为某个合法的 TPM 所拥有。

5.2.4 密钥管理

1．种类和用途

根据密钥的使用范围，平台中的密钥可以分为三类：

平台身份类密钥，如密码模块密钥 EK（Endorsement Key）、平台身份密钥 PIK（Platform Identity Key）、平台加密密钥（Platform Encryption Key）；平台存储类密钥，如存储主密钥（Storage Master Key， SMK）；用户类密钥（User Key，UK）。

密钥种类如表 5-1 所示。

表 5-1 密钥种类

平台身份类密钥	密码模块密钥（EK）
	平台身份密钥（PIK）
	平台加密密钥（PEK）
平台存储类密钥	存储主密钥（SMK）
用户类密钥	用户密钥（UK）

1）密码模块密钥 EK：是可信密码模块的初始密钥，是平台可信度的基本元素。

2）平台身份密钥 PIK：是可信密码模块的身份密钥。平台身份密钥用于对可信密码模块内部的信息进行数字签名，实现平台身份认证和平台完整性报告。

3）平台加密密钥 PEK：与平台身份密钥配对构成双密钥（及双证书）。平台加密密钥可用于平台间的密钥迁移以及平台间的其它数据交换。

4）存储主密钥 SMK：用于保护平台身份密钥 PIK 和用户密钥 UK 的主密钥。

5）用户密钥 UK：用于实现用户所需的密码功能，包括保密性、完整性保护和身份认证等。

2．密钥存储保护

密码模块密钥、存储主密钥、平台所有者的授权数据直接存放在可信密码模块内部，通过可信密码模块的物理安全措施保护。

平台身份密钥、平台加密密钥、用户密钥等可以加密保存在模块外部。

平台通过设置密钥实体的权限数据来控制用户对密钥的访问。权限数据必须被加密存储保护。

3．密钥的生命周期

平台生命周期可以分为以下几个阶段

1）制造。包括可信密码模块生产、集成和计算机系统的制造过程。

2）初始化。取得平台所有者权限过程。

3）部署。平台所有者将平台部署到应用系统的过程。

4）应用。平台用户使用平台完成平台完整性度量、平台身份证明和数据安全保护的过程。

5）撤销。即平台的销毁过程。

在平台的生命周期中，各种密钥的生成、使用和销毁过程如表 5-2 所示。

表 5-2 密钥的生成、使用和销毁过程

	制造	初始化	部署	应用	撤销
密码模块密钥	生成	重新生成、使用			销毁
平台身份密钥			生成	生成、使用	销毁
平台加密密钥			生成	生成、使用	销毁

存储主密钥		生成	使用		销毁
用户密钥				生成、使用、迁移	销毁

5.2.5 证书管理

平台设置密码模块证书和平台证书两种数字证书。平台证书采用“双证书”机制，平台证书包含平台身份证书和平台加密证书，平台身份证书用于平台身份的证明，平台加密证书执行加密运算，用于平台间密钥迁移以及其它敏感数据的交换保护。

1．密码模块证书

1）证书的签发：密码模块证书可以在平台的生产阶段由可信方颁发，也可以在平台的部署阶段由用户委托可信方颁发。

2）证书的使用：密码模块证书用于建立密码模块密钥与可信密码模块的绑定关系。平台一旦确定了所有者，必须在取得所有者授权后才可以访问该证书，以保护平台所有者的隐私。

3）证书的撤销：密码模块证书的有效期是可选属性。密码模块证书一般不需要更新，但是很多因素可能引起证书的撤销和废止，例如，平台弃用或丢失，重新生成密码模块密钥等。

4）证书的内容：密码模块证书为公钥证书，符合 X.509 V3 标准。包含的具体内容如表 5-3 所示。

表 5-3　密码模块证书包含的内容

字段名	描述	字段状态
证书类型标签	用以区分其它证书类型	必须
密码模块密钥对的公钥	可信密码模块密钥对的公钥值	必须
可信密码模块型号	生产商定义的信息	必须
规范版本号	标识该可信密码模块所遵循的规范	必须
证书发布者	标识该证书的发布者	必须
签名值	签发者对证书的签名值	必须
可信密码模块声明	与可信密码模块安全相关的声明	可选
有效期	证书的有效期限	可选
相关策略	相关策略	可选
撤销定位	标识撤销状态信息的查询位置	可选

2．平台证书

平台证书采用“双证书”机制，包含平台身份证书和平台加密证书。

1）证书的签发。平台身份证书和平台加密证书签发实体必须是可信方。证书生成要求如下：

（1）平台身份证书的 ECC 密钥对在可信密码模块内部生成。

（2）平台加密证书的 ECC 密钥对由密钥管理中心（KMC）生成，用安全方式传送给平台。

（3）可信方为平台签发平台身份证书和平台加密证书。

（4）平台解密得到平台身份证书和平台加密证书，以及平台加密密钥的私钥。

2）证书的使用。平台身份证书的用途是验证平台身份密钥（PIK）私钥对 PCR 值的签名；平台加密证书用于平台间密钥迁移以及其它数据的交换。

3）证书的撤销和废止。以下几种情况可能引起平台身份证书的撤销：

（1）密码模块密钥或平台身份密钥的安全性受到威胁。

（2）密码模块证书被撤销。

（3）证书签发实体的签名根密钥丢失。

（4）密码模块证书和平台身份证书间的联系暴露。

（5）与同一个密码模块证书关联的平台身份证书间的联系暴露。

如果证书被撤销，证书签发实体应及时发布证书的状态以供验证者查询。

4）证书的内容。平台身份证书包括平台身份密钥（PIK）的公钥和证书签发者认为必要的信息，符合 X.509 V3 标准。包含的具体内容如表 5-4 所示。

除“密钥用途”属性外，平台加密证书的信息与平台身份证书一致。

表 5-4　平台身份证书包含的内容

字段名	描述	字段状态
证书类型标签	用以区分其它证书类型	必须
PIK 的公钥	平台身份密钥对的公钥值	必须
可信密码模块型号	生产商定义的信息	必须
规范版本号	标识该可信密码模块所遵循的规范	必须
证书发布者	标识该证书的发布者	必须
密钥用途	标识密钥的用途	必须
签名值	签发者对证书的签名值	必须
身份标签	由发布者给出的与 PIK 相关的字符串	必须
有效期	证书的有效期限	可选
相关策略	相关策略	可选
撤销定位	标识撤销状态信息的查询位置	可选

5.3　可信平台控制模块

可信平台控制模块是可信应用的核心控制模块，它为可信应用提供物理上的三个根功能：可信度量根、可信报告根与可信存储根。以可信平台控制模块为基础，可以扩展出可信计算平台的可信度量功能、可信报告功能与可信存储功能。

可信平台控制模块可以直接读取与之相连的身份识别设备的信息，获取当前操作用户的相关资料，作为可信应用处理事务的重要依据之一。

在计算机主板上，主板芯片组通过 LPC 总线与模块相连，并通过 LPC 总线向可信平台控制模块发送指令和读取应答信息，从而完成一系列的可信应用操作。

5.3.1　体系结构

在 TPCM 内部应包括如下单元：微处理器、非易失性存储单元、易失性存储单元、随机数发生器、密码算法引擎、密钥生成器、定时器、输入输出桥接单元和各种输入输出控制器模块，如图 5-5 所示。

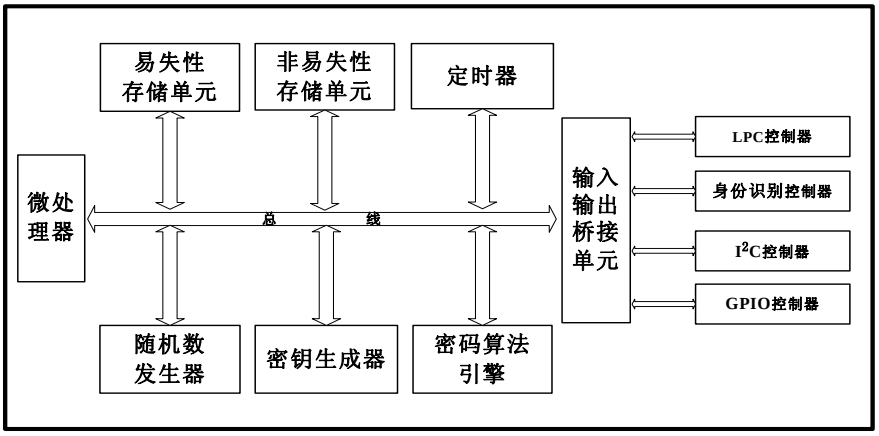


图 5-5　TPCM 原理框图

非易失性存储单元、易失性存储单元、随机数发生器、密码引擎、密钥生成器和定时器统一映射到片内微处理器的访问地址空间。在地址访问方面，设计者自行定义他们在地址空间中的映射关系。

5.3.2　主要功能

可信平台模块实现了可信度量、可信存储和可信报告三大基本功能，实现可信平台用户管理、可信平台控制模块内部固件和可信平台控制模块内部维护管理三个辅助功能。下面将针对完整性度量、存储和报告三个主要功能进行详细阐述。

1．完整性度量

使用杂凑算法对被度量对象计算其杂凑值的过程。TPCM 采用主动方式对可信计算平台中软件、固件或硬件部件特征数据进行散列运算，所得到的结果即为该部件的完整性度量值。在计算机启动过程中使用扩展度量模块(EMM，Extended Measurement Module)作为代码度量执行部件组，实现对后续执行代码的完整性度量和信任链扩展。根据其在系统中的启动顺序，分为 EMM1、EMM2 和 EMM3 三个执行部件。

完整性度量流程要求：

1) TPCM 上电，完成初始化后，将 Boot ROM 中的 EMM1（位于 BIOS 内部的，负责对 EMM2 进行度量的代码）读入到 TPCM 中。作为可信起点的可信度量模块通过调用散列运算的硬件引擎，对读入的 EMM1 执行扩展散列运算，将生成的散列值和日志临时存储于 TPCM。
2) 当 RTM 模块对 EMM1 度量工作完成后，TPCM 发送控制信号，平台开始上电，从而构建以 EMM1 为当前系统控制和执行部件的可信执行环境。
3) 发出控制信号后，TPCM 进入指令等待状态，并可以接受可信计算平台发出的指令。
4) 在完整性度量剩余阶段中，TPCM 可以响应可信计算平台发出指令，将散列运算结果和日志存储到 TPCM 中。

2．完整性存储

可信平台控制模块也是可信计算平台的完整性存储根，必须实现对平台内部数据的安全存储。

TPCM 将散列运算结果作为度量值结果存到指定平台配置寄存器（PCR）中，PCR 是可信平台控制模块内部用于存储平台完整性度量值的存储单元。同时必须指定是覆盖存储或是递加存储方式。如覆盖存储，则直接将散列运算结果存入指定 PCR，如递加存储，则将散列运算结果拼接到目标 PCR 的已有存储值之后，再进行散列运算，然后将所得结果再存储于该 PCR 中。

同一个 PCR 可以存储多个部件的递加完整性度量值，也可以存储一个部件的多次递加完整性度量值。若一个 PCR 中要存储多个部件的递加完整性度量值，则从第一个部件开始，将该部件完整性度量值拼接到目标 PCR 的已有存储值之后，再进行散列运算，然后将所得结果再存储于该 PCR 中，依次递推，最后一个部件的完整性度量值存储操作完成后，所得 PCR 的值即为度量的一系列部件的完整性度量值，同时还存储了度量的先后顺序。同一个部件的前后多次递加完整性度量值也采用前述类似的链接方式存储在 PCR 里。

3．完整性报告

TPCM 可向外部实体提供完整性度量值报告的功能，所报告的度量值作为判断可信计算平台可信性的依据。

接收到报告完整性度量值指令后，TPCM 使用平台身份密钥应对完整性度量值进行数字签名，然后再返回给外部实体。

5.4 可信平台主板

可信平台控制模块安装在可信主板上。可信主板构成了可信计算的舞台。可信计算主板涉及的功能主要包括信任链的建立，附加有可信安全硬盘存储等功能。可信链的建立基于可信度量，可信度量的方法是代码的完整性度量。完整性度量功能检查运行前后软硬件代码的一致性，从而保证代码不被外部篡改。

5.4.1 体系结构

可信计算平台主板是由TPCM和其它通用部件组成，以TPCM自主可信根（RT）为核心部件实现完整性度量和存储机制，并实现平台可信引导功能。

主板主要组成部件包括：可信平台控制模块TPCM，中央处理器CPU、随机存取存储器（RAM）、视频显示控制器、外部辅助存储器、用户输入输出接口（I/O）与设备、BIOS/UEFI BIOS等BootROM固件、操作系统装载器和操作系统内核等，如图5-6所示：

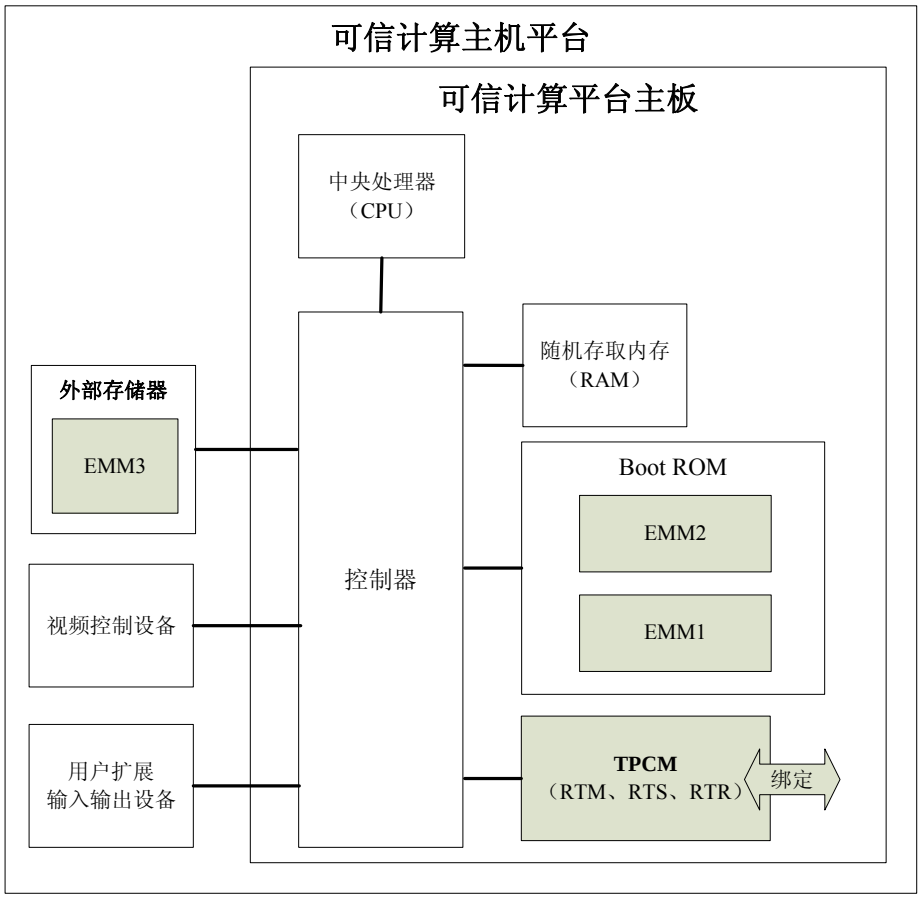


图5-6　可信计算平台主板组成结构

- 可信平台控制模块（TPCM）：包括 TPCM 物理硬件与嵌入系统，以及对外提供的驱动程序等实体组成。
- 可信计算平台主板是基于 TPCM 模块的计算机主板，包括 CPU、动态存储器、显示控制器、TPCM 硬件设备、BootROM 固件层支撑模块及其设备驱动程序和 TPCM 嵌入式系统等实体。
- 计算机主板构建原则需确保 TPCM 模块与主板的一一对应绑定关系。TPCM 与计算机主板其它部件的协作关系上应满足如下要求：TPCM 先于计算机主板其它部件启动，包括 CPU，为实现 RTM 度量 Boot ROM 的起始代码 EMM1 构造必要条件；TPCM 能够通过物理电路连接，可靠地读取主机 BIOS/EFI BIOS 的初始引导代码 EMM1，并对其实施完整性度量和存储操作；扩展度量模块 EMM 代理 RTM 度量平台代码的装载过程，通过功能接口访问 TPCM。
- 可信根（RT）：TPCM 模块实体是主板平台的可信根，包括：可信度量根（RTM）、可信存储根（RTS）和可信报告根（RTR）。
- 可信度量根（RTM）：TPCM 嵌入式系统中用于度量 BootROM 程序中的 Boot Block 或一段程序代码的执行部件。
- 可信存储根（RTS）：维护完整性摘要的值和摘要序列的加密引擎和加密密钥。
- 可信报告根（RTR）：报告可信计算平台寄存器（PCR）所持有数据的计算引擎和加密密钥。

- 扩展度量模块（EMM）：接受了完整性度量检查并被装载到当前执行环境中，度量后续代码装载的部件。作为 RTM 度量引擎的扩展度量模块，实现对执行部件的完整性度量，确保信任传递。
- EMM1：通过 RTM 对其完整性度量并被装载到系统的一段 BootROM 初始引导程序，作为主板开机引导中装载执行部件对 Boot ROM 其它部件执行完整性度量的扩展度量模块。
- EMM2（BIOS/UEFI）：通过 EMM1 对其完整性度量，并被装载的扩展度量模块实体，负责对操作系统装载器进行完整性度量与可信装载的一段 Boot ROM 程序。
- EMM3：存储于外部存储器中用来装载操作系统内核的执行部件，通过 EMM2 对其进行完整性度量并被完整性装载到主板系统中，对被装载的操作系统内核执行完整性度量的扩展度量模块。

信任链上主要部件之间的相互协作关系是：RTM 度量 EMM1，EMM1 度量 EMM2，EMM2 度量 EMM3，EMM3 度量操作系统内核；可信计算主板以 RTM、EMM1、EMM2 和 EMM3 为节点搭建信任链传递。

5.4.2 主要功能

1．信任链建立

信任链从开机到操作系统内核装载之前的建立过程应满足如下要求：TPCM作为信任链的信任根，EMM作为度量代理节点，通过完整性度量，实现信任传递与扩展。信任链建立的一般流程如图5-7所示：

a) TPCM 先于 Boot ROM 被执行前启动，由 TPCM 中的 RTM 度量 Boot ROM 中的初始引导模块（Boot Block），生成度量结果和日志，并存储于 TPCM 中；
b) TPCM 发送控制信号，使 CPU、控制器和动态存储器等复位；平台加载并执行 Boot ROM 中的 Boot Block 代码；
c) Boot Block 中的 EMM1 获得系统执行控制权，信任从 RTM 传递到 EMM1；
d) EMM1 度量 Boot ROM 版本信息和 Main Block 中的 EMM2 代码；EMM1 存储度量结果到 TPCM 中的 PCR，存储度量日志到 Boot Block 中；
e) 平台加载并执行 Main Block 的代码；
f) Main Block 中的 EMM2 获得系统执行控制权，信任从 EMM1 传递到 EMM2；
g) EMM2 将在 a)步骤中存储在 TPCM 中的日志存储到 ACPI 中；EMM2 将在 d)步骤中存储在 Boot Block 中的日志存储到 ACPI 中；EMM2 度量平台启动部件，包括显示卡、硬盘、网卡等外部设备；在完成对平台启动部件度量后，EMM2 度量存储在外存中的操作系统装载器（OS Loader）；EMM2 生成对平台启动部件和 OS Loader 的度量结果和日志，度量结果存储到 TPCM 的 PCR 中，度量事件日志保存到 ACPI 中；
h) 平台加载并执行 OS Loader 的代码；
i) OS Loader 中的 EMM3 获得系统执行控制权，信任从 EMM2 传递到 EMM3；
j) EMM3 度量操作系统内核，生成度量结果和日志，度量结果存储到 TPCM 的 PCR 中，度量事件日志保存到 ACPI 中；
k) 平台加载并执行 OS Kernel 的代码；
l) OS Kernel 中的 EMM4 获得系统执行控制权，信任从 EMM3 传递到 EMM4；

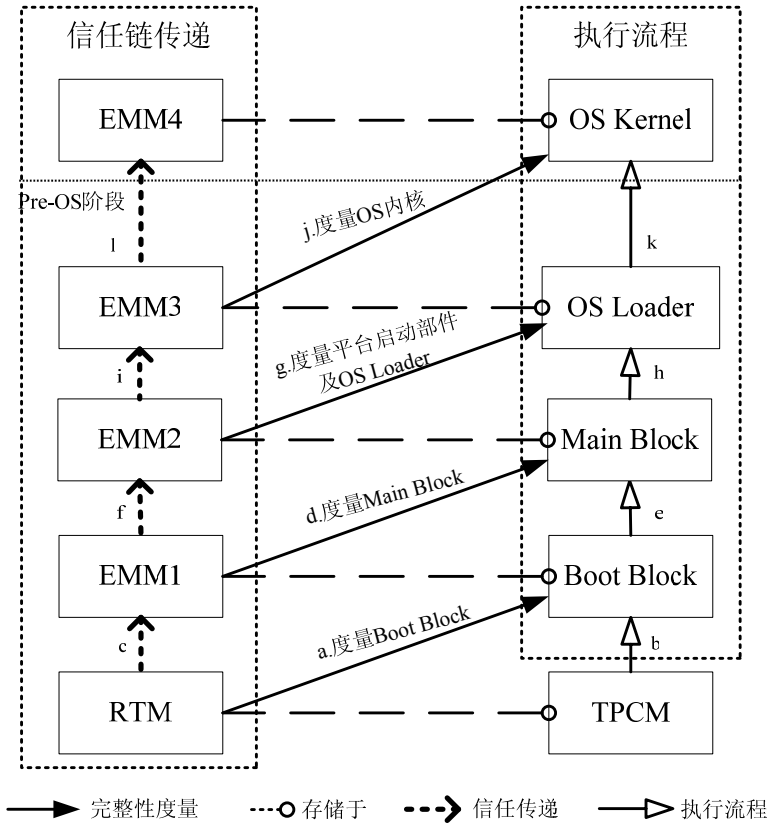


图5-7　主板引导过程部件信任传递关系网络和信任链建立流程

2．完整性度量

信任链基于可信度量根RTM建立，通过扩展度量模块EMM实现信任传递。RTM和EMM采用杂凑算法对部件代码进行完整性计算，并存储度量结果，实现完整性度量。一次完整的度量流程如图5-8所示。

完整性度量流程：

a) RTM或者EMM使用杂凑算法对“部件i”的二进制代码进行计算；

b) RTM或者EMM生成在第a)步中对“部件i”的计算结果“度量事件i描述”；该描述包括杂凑算法的结果，“度量值i”，以及本次度量事件的上下文信息“度量事件i上下文”。

c) RTM或者EMM通过接口调用TPCM，将“度量值i”扩展存储到预先定义与部件i相关的PCR[i]中。

d) RTM或者EMM将“度量事件i描述”存储于度量事件日志中。

完成上述四个步骤的整个过程为一次完整性度量事件。

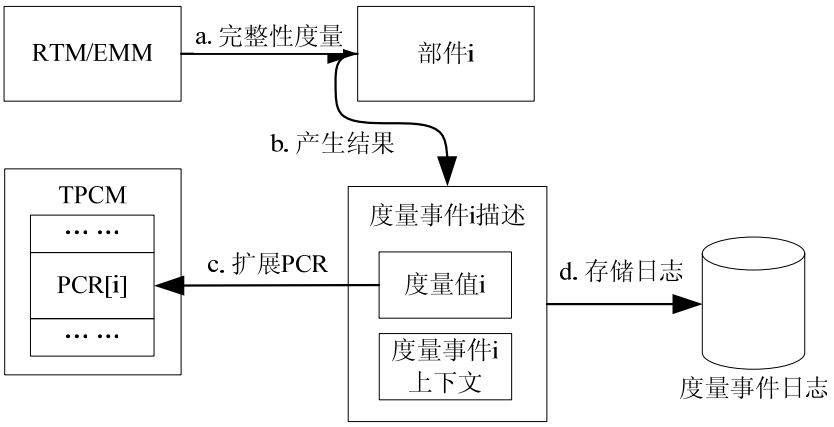


图5-8　完整性度量流程图

5.5　可信基础支撑软件

可信基础支撑软件（TBSS，Trusted Basic Supporting Software）是可信计算平台支撑体系中的基础软件部分，能够保障信任链在软件系统的传递，保证系统软件的可信性，为应用开发提供必要的标准编程接口，管理可信计算平台的可信资源。可信基础支撑软件是可信计算的核心。

5.5.1　软件框架

可信基础支撑软件运行于可信平台控制模块之上，由可信软件基 TSB（Trusted Software Base）、可信基础支撑软件系统服务（TSS，TBSS System Service）和可信基础支撑软件应用服务 TAS（Trusted Application Service）三个部分组成，向可信计算平台上层应用提供完整性、数据保密性和身份认证管理功能的标准接口，其体系结构如图 5-9 所示。

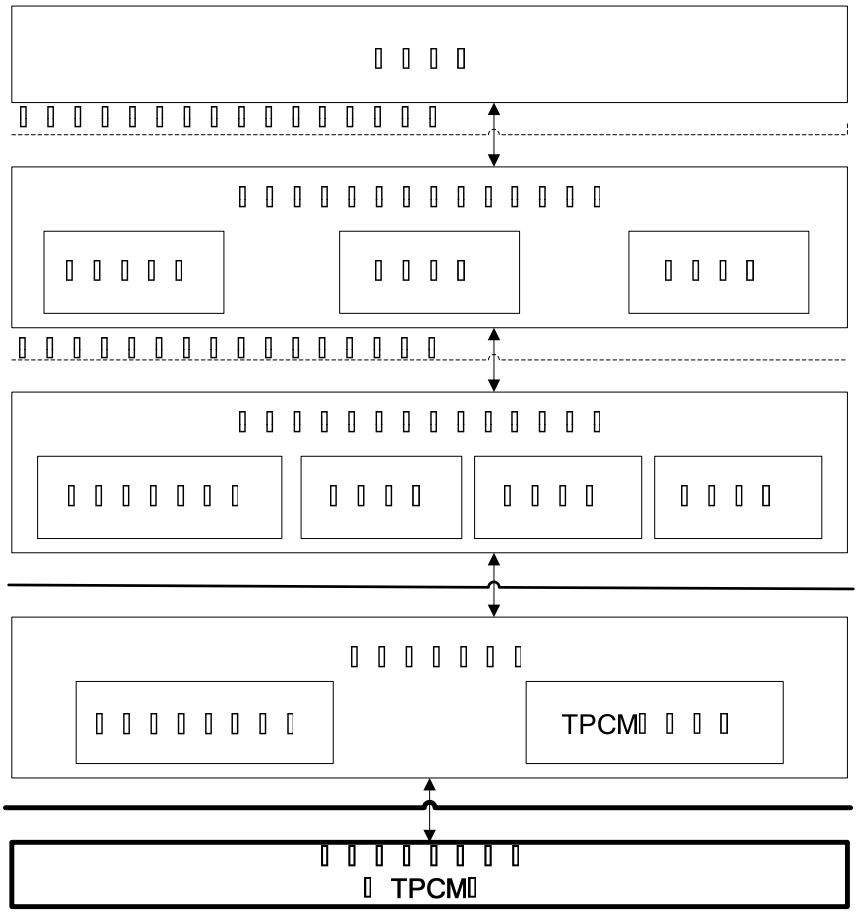


图5-9　可信基础支撑软件架构图

可信基础支撑软件分为以下三个层次：

1) 可信软件基：包含在操作系统内核中，由可信访问控制模块和 TPCM 驱动模块组成。本部分应实现对操作系统内核之上的重要系统软件和用户要求的应用程序进行完整性度量，完成操作系统之上的信任链传递，保证其符合系统规定的完整性要求。可信软件基还可以为可信计算基在软件部分提供完整性方面的保证，并通过信任链传递，保证可信计算基各部分之间的相互信任。
2) 可信基础支撑软件系统服务：处于系统服务层，通过 TPCM 驱动接口与可信软件基交互，向应用程序提供 TPCM 的证书，密钥，密码功能和完整性数据管理四类接口。
3) 应用层的可信基础支撑软件应用服务：处于应用服务层，向用户提供完整性保护、可信认证、数据保护三类应用服务接口。

5.5.2　主要功能

为了使用户安全、有效的使用可信计算功能，可信基础支撑软件应提供完整性、数据保密性管理和身份认证管理功能。

1．完整性管理功能

可信基础支撑软件应向用户提供统一的完整性管理框架，对基于可信计算平台的软硬件系统的完整性状态进行度量、存储与报告，保护可信计算平台的应用环境不被篡改。

对可信计算平台完整性状态的度量是基于可信链传递而实现，即从可信度量根RTM开始，逐级向上度量软件系统引导程序、系统软件和应用程序的完整性。可信基础支撑软件必须基于可信软件基对系统软件进行强制度量，并应用户要求对相应应用程序进行度量。

完整性度量即获取可信计算平台软硬件系统的完整性度量值，并将这些值记录到PCR中的过程。

完整性状态数据分为两种：存储在PCR中的完整性度量值；以及相应的可信计算平台的软硬件系统完整性日志。

完整性存储是可信基础支撑软件对可信计算平台软件系统的完整性日志进行存储管理的过程。

可信基础支撑软件应对根据用户要求，将操作系统和相关应用程序的度量值与完整性预期值存储库中的厂商预存的完整性度量值进行比较验证，将结果报告给用户。

2．数据保密性管理功能

数据保密性管理应向用户提供相应框架管理敏感数据，防止机密信息在未经授权的情况下泄漏。本部分可以选择在内核态，或用户态，或结合两者共同实现。

3．身份认证管理功能

身份认证管理应向用户提供相应框架管理用户权限和可信计算平台的相关证书，用于在应用中认证用户和平台身份的可信性，本部分应结合内核态和用户态实现。

身份认证管理应通过管理使用可信计算平台的本地用户身份与可信硬件的绑定关系，保证用户身份的可信性。

与可信计算平台交互的远程用户应能通过可信证书验证可信计算平台以及相关用户身份,身份认证管理应保障相关证书的存储与使用。

5.6　可信网络连接

可信网络连接（TNC，trusted network connection）是指终端连接到受保护网络的过程，包括用户身份鉴别、平台身份鉴别、平台完整性校验三个步骤。

终端在接入网络之前，对其进行用户身份认证、平台身份认证和平台完整性度量，只有满足安全策略的终端才被允许接入网络中，使得具有潜在威胁的终端不能直接接入网络，这是一种主动的、预先防范的方法。可信网络连接架构是可信计算体系结构的一个重要组成部分，是具有可信平台控制模块的终端接入计算机网络的架构，目的是使信任链从终端扩展到网络，将单个终端的可信状态扩展到互联系统。

5.6.1　体系结构

可信网络连接架构规定具有 TPCM 的终端与计算机网络的可信网络连接，其架构图如图 5-10 所示：

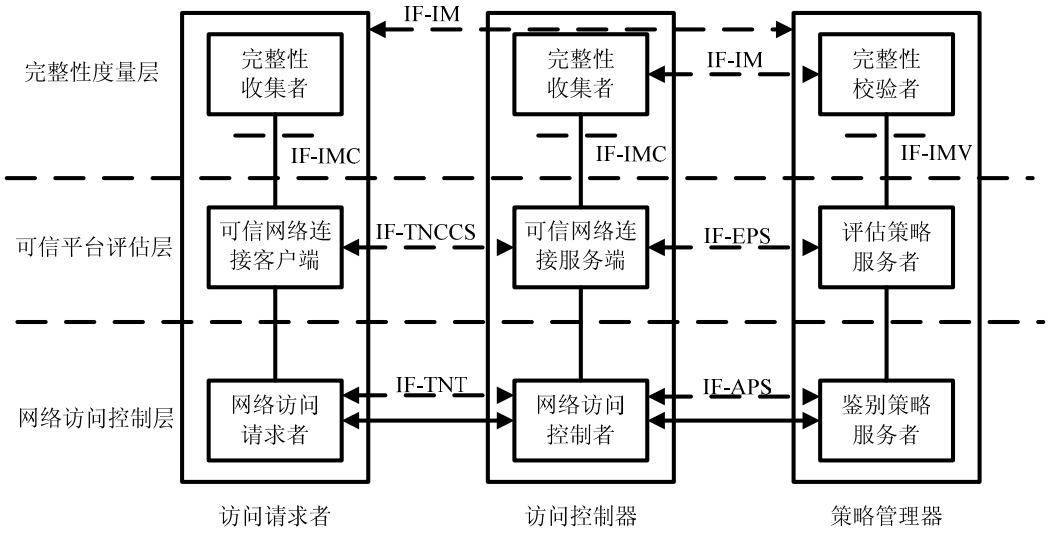


图5-10　可信网络连接架构

上图所示的可信网络连接架构中，存在三个实体：访问请求者、访问控制器和策略管理器，从上至下分为三个层次：完整性度量层、可信平台评估层和网络访问控制层。

访问请求者 AR（Access Requestor）：访问请求者是请求接入受保护网络的实体，功能为发出访问请求，完成与访问控制器的双向用户身份鉴别；收集完整性度量值并发送给访问控制器，完成与访问控制器之间的双向可信平台评估，依据策略管理器在用户身份鉴别和可信平台评估过程中生成的结果执行访问控制。该实体包括以下组件：网络访问请求者、可信网络连接客户端和完整性收集者。

访问控制器 AC（Access Controller）：访问控制器是控制访问请求者访问受保护网络的实体，功能为完成与访问请求者之间双向用户身份鉴别和可信平台评估；接收访问请求者的完整性度量值，收集自身的完整性度量值，将这些完整性度量值发送给策略管理器；依据策略管理器在用户身份鉴别和可信平台评估过程中生成的结果执行访问控制。该实体包括以下组件：网络访问控制者、可信网络连接接入点和完整性收集者。

策略管理器 PM（Policy Manager）：策略管理器负责制定可信平台评估策略，协助访问请求者和访问控制器实现双向用户身份鉴别，验证访问请求者和访问控制器的 PIK 证书有效性，校验访问请求者和访问控制器的平台完整性，生成访问请求者和访问控制器在用户身份鉴别过程和可信平台评估过程中的结果。该实体包括以下组件：鉴别策略服务者、评估策略服务者和完整性校验者。

网访问请求者和访问控制器都具有 TPCM，访问请求者请求接入保护网络，访问控制器控制访问请求者对保护网络的访问。策略管理器对访问请求者和访问控制器进行管理。

在网络访问控制层，网络访问请求者、网络访问控制者和鉴别策略服务者执行用户身份鉴别协议，实现访问请求者和访问控制器之间的双向用户身份鉴别。

在可信平台评估层，可信网络连接客户端、可信网络连接服务端和评估策略服务者执行可信平台评估协议，实现访问请求者和访问控制器之间的双向可信平台评估（包括平台身份鉴别和平台完整性校验）。在可信平台评估过程中，若平台身份未成功鉴别，则断开连接；否则，验证平台完整性校验是否成功通过。若平台完整性校验未成功通过，则接入隔离域对终端平台进行修补，修补后可重新进行可信平台评估过程；否则，访问请求者接入保护网络。

在完整性度量层，完整性收集者收集访问请求者和访问控制器的平台完整性度量值，完整性校验者校验这些平台完整性度量值，并通过 IF-IMC 和 IF-IMV 接口为可信平台评估层服务。

上述用户身份鉴别协议和可信平台评估协议都是基于可信方策略管理器的双向对等鉴别协议，称为三元对等鉴别协议。网络访问控制层执行 TePA-AC，网络访问请求者和网络访问控制者依据用户身份鉴别结果和可信平台评估层发送的连接决策执行端口控制，从而实现访问控制。

5.6.2　主要功能

可信网络连接通过访问请求者、访问控制器以及策略管理器三个实体来实现访问请求、访问控制以及策略管理的功能。下面主要针对这三者进行介绍。

1．访问请求者

访问请求者是请求接入受保护网络的实体，功能为发出访问请求，完成与访问控制器的双向用户身份鉴别；收集完整性度量值并发送给访问控制器，完成与访问控制器之间的双向可信平台评估，依据策略管理器在用户身份鉴别和可信平台评估过程中生成的结果执行访问控制。

该实体包括以下部件：网络访问请求者、可信网络连接客户端和完整性收集者。

1）网络访问请求者

负责向访问控制器发起访问请求，与网络访问控制者和鉴别策略服务者执行用户身份鉴别协议以实现访问请求者和访问控制器在网络访问控制层上的双向用户身份鉴别。

负责向访问控制器和策略管理器转发上层协议数据。

依据鉴别策略服务者生成的用户身份鉴别结果以及可信网络连接客户端生成的连接决策，对自身的端口进行控制，实现对访问控制器的连接控制。

2）可信网络连接客户端

通过IF-IMC接口向完整性收集者请求并接收完整性度量值，与可信网络连接接入点和评估策略服务者执行可信平台评估协议，实现访问请求者和访问控制器的双向可信平台评估。

依据评估策略服务者生成的可信平台评估结果生成连接决策并发送给网络访问请求者。

3）完整性收集者

利用可信计算平台所提供的完整性服务收集访问请求者和访问控制器的平台完整性信息。

2．访问控制器

访问控制器是控制访问请求者访问受保护网络的实体，功能为完成与访问请求者之间双向用户身份鉴别和可信平台评估；接收访问请求者的完整性度量值，收集自身的完整性度量值，将这些完整性度量值发送给策略管理器；依据策略管理器在用户身份鉴别和可信平台评估过程中生成的结果执行访问控制。

该实体包括以下部件：网络访问控制者、可信网络连接接入点和完整性收集者。

1）网络访问控制者

负责激活网络访问控制层的用户身份鉴别协议，与网络访问请求者和鉴别策略服务者执行用户身份鉴别协议以实现访问请求者和访问控制器的双向用户身份鉴别。

负责向访问请求者和策略管理器转发可信平台评估层的协议数据。

依据鉴别策略服务者生成的用户身份鉴别结果以及可信网络连接接入点生成的连接决策，对自身的端口进行控制，实现对访问请求者的接入控制。

2）可信网络连接接入点

负责激活可信平台评估层上的可信平台评估协议，通过IF_IMC（见5.5.6）接口向完整性收集者请求并接收完整性度量值，与可信网络连接客户端和评估策略服务者执行可信平台评估协议，实现访问请求者和访问控制器的双向可信平台评估。

依据评估策略服务者生成的可信平台评估结果生成接入决策并发送给网络访问控制者。

3）完整性收集者

与 1 中 3）相同。

3．策略管理器

策略管理器负责制定可信平台评估策略，协助访问请求者和访问控制器实现双向用户身份鉴别，验证访问请求者和访问控制器的PIK证书有效性，校验访问请求者和访问控制器的平台完整性，生成访问请求者和访问控制器在用户身份鉴别过程和可信平台评估过程中的结果。

该实体包括以下部件：鉴别策略服务者、评估策略服务者和完整性校验者。

1）鉴别策略服务者

与网络访问请求者和网络访问控制者执行用户身份鉴别协议，并作为该协议中的可信方，实现访问请求者和访问控制器之间的双向用户身份鉴别。

2）评估策略服务者

与可信网络连接客户端和可信网络连接接入点执行可信平台评估协议，并作为该协议中的可信方，实现访问请求者和访问控制器的双向可信平台评估。

评估策略服务者验证访问请求者和访问控制器的平台身份证书的有效性，平台身份证书有效性确认后，通过IF-IMV接口向完整性校验者发送访问请求者和访问控制器的平台完整性度量值，并接收由完整性校验者返回的访问请求者和访问控制器的平台完整性度量值的校验结果，最后生成可信平台评估结果（平台身份证书有效性验证结果和平台完整性校验结果）发送给访问请求者和访问控制器。

3）完整性校验者

利用完整性管理中的平台部件的完整性基准值校验访问请求者和访问控制器的平台完整性信息。

5.6.3 远程证明

传统网络应用根据远程访问者的身份实施访问控制，不考虑远程操作平台运行环境的可信性。如果访问者拥有敏感信息的访问权，但敏感信息在一个不可信的平台上处理，仍然会存在非法传播的可能。所以，在身份认证的基础上加入远程平台运行环境的可信性认证十分必要。下面主要介绍在可信网络连接中的远程证明技术。

在可信计算平台的远程证明过程中，平台通过可信的度量代理对指定的状态进行度量，并将度量结果提交给 TPM，TPM 通过其由硬件保护的私钥（Attestation Identity Key，AIK）对度量结果加以签名，向第三方证明度量结果的来源真实性和完整性。

TPM 内部有一组 PCR（Platform Configuration Register）寄存器，每个 PCR 可以被定义只与计算平台的某一类系统特定事件状态相关。每次相关事件发生时，计算平台将事件记录结果保存，并将记录结果的 Hash 值扩充到 TPM 中事件对应的 PCR 中[50][51][52][53]。将 Hash 值 R 扩充到 PCR[n]中的过程为 PCR[n]=hash（PCR[n]+R）。显然，PCR 值与事件历史过程相关，并与事件记录的顺序有关，因此它们的值实际反映了事件发生的顺序历史。

TCG 的远程证明步骤如下：

1） 质询方要求证明平台提交相关的事件记录日志及对应的 PCR 值；
2） 平台代理采集相关的 SML；
3） 平台代理从 TPM 获得 PCR 值；
4） TPM 用 AIK 私钥对 PCR 值进行签名；
5） 平台代理获取 TPM 本身的证明证书，随后将签名后的 PCR 值、SML 项及证书提交给质询方；
6） 质询方对度量报告进行验证。质询方对度量结果计算其摘要值并和 PCR 进行比对，对 TPM 证书及其签名进行验证。

5.7 可信计算的应用

可信计算的应用正方兴未艾。本节将从可信计算平台以及可信网络连接两个方面举例介绍可信计算技术的主要应用场景。

5.7.1 可信计算平台应用场景

可信计算平台产品方面，TCG发展势头迅猛，其研究领域已从个人计算机迅速扩展到服务器、PDA、手机等各类信息平台。据IDC预测，至2007年，将有70％的PC集成TCG技术。可以预见TPM将成为未来包括台式机、笔记本、移动终端等设备的标配。目前，美国IBM、HP公司已有大量可信PC机和笔记本电脑出售。

在可信平台的基础上，客户机和服务器能够互相验证对方的软件状态，可以应用于许多场境，包括风险管理、资源管理、电子商务、电子政务（政府信息系统）、生产信息系统、安全监控和紧急响应。

自主创新的可信计算平台和相关产品作为国家信息安全基础建设的重要组成部分，实质上是国家信息安全战略的重要部分。只有掌握关键技术才能摆脱牵制，提升我国整个信息安

全的核心竞争力。可信计算平台产品将会在政府、机关、军队、金融等各个领域中发挥出非凡的作用。

1．政府信息系统领域

政府综合信息系统网络分为系统内网、电子政务专网和Internet外网三个部分，可以采用可信计算平台产品解决政府综合信息系统的安全管理问题，以解决节点安全为基础，通过网络信任管理系统的强制身份认证、授权访问控制和责任审计，拓展到综合信息系统的安全管理，从而保证用户可信、终端可信乃至整个网络安全可信及应用可信，在保证安全前提下实现互连互通，并为政府综合信息网的接入提供灵活的安全接入和管理方式。

在政府信息系统的建设和使用中，通过应用可信计算技术，政府机构可以更加放心地借助计算机和计算机互联网络来处理各种业务，提高办事效率，改善政府形象，提升政务水平和服务能力。

应用可信计算技术，可以更安全地存储、处理、传输和共享敏感信息和数据。即使硬件丢失或被盗，存放在其中的信息也还能够保持秘密。基于可信计算技术的数据保护功能可以被广泛地应用于重要的涉密单位和部门。这些部门最重要的信息安全需求就是信息的保密性和信息流的安全保密控制。敏感涉密信息应被预先确定某个范围，只有在这个预先确定的范围内敏感信息可以以明文方式呈现，即敏感涉密信息只能限制在特定的平台和系统内部流动。可信计算技术的数据保护功能可以很安全地满足这一需求。在一些安全密级较高的单位，信息流安全保密控制解决方案可以使得这些部门无需为了信息保密而单独建网，不同密级的信息及存储和处理平台可以共同存在同一网络中，这样在保证信息安全保密的条件下，不仅可以降低系统复杂度，还可以减少建设和使用成本。

同时，应用可信计算技术，政府可以加强对其所拥有信息系统的管理控制力度，降低管理成本，提高信息安全水平。政府信息系统可以对试图接入或访问其资源的平台和人员，包括内部人员和外部合作单位或人员，进行安全状态和身份的审核，获得其相关安全信息，判断其是否符合系统安全策略，从而进一步决定它的网络资源访问权限，这些网络资源包括政府部门的网络服务和信息等。

总之，可信计算技术可以极大地提高信息安全的水平，而信息安全水平的提高则可以促进政府的信息化建设，从而提高整个社会的信息化水平，减少信息孤岛，降低社会成本，提高社会效能。

2．金融信息系统领域

金融行业信息系统的安全监管系统、生产系统、办公系统、网银系统和外单位接入系统等都要求保证系统内节点可信安全，接入部分可信安全。采用可信计算平台产品，实现用户可信，终端可信，局域网可信，网络互联可信，最终实现整个金融行业信息系统的安全可信，金融行业信息系统中的所有用户、终端及服务器都必须经过可信认证，并纳入可信可控管理，对资源实施授权访问控制，避免信息资源的非法使用，对行为进行安全责任审计，减少内部安全隐患的发生。

电子商务信息系统的主要模式是基于服务器/客户端多层体系结构的网络应用系统，其安全需求主要集中保护应用服务网络系统的可信安全和交易过程中双方的身份验证，交易信息的安全传输以及用户私密信息的安全保护。在电子商务信息系统的安全方面重点考虑保护应用服务网络系统的可信安全，采用可信计算平台，部署可信服务器和软硬件结合的可信计算产品和网络信任管理系统，在应用服务网络中对电子商务的数据服务器、应用服务器进行重点保护，对接入服务网络的集团用户按照会员身份进行可信可控接入管理，并对信息资源进行授权访问控制，同时，在交易信息传输安全和对交易双方身份认证方面，采用相应的安全通信协议，保证交易的保密性、完整性、抗抵赖和防伪冒。

3．企业信息系统领域

企业一般通过人员管理制度来规定合法信息的使用，传统上，由信息安全技术提供的支持十分有限。利用可信计算技术的安全存储和密钥保护技术，企业可以将敏感信息限制并绑定在一个特定部门所在的系统内，敏感涉密信息只能在指定系统内部以明文方式被访问和利用，一旦离开指定的系统范围，敏感涉密信息就表现为不可解读的密文。

同时，可信计算技术的数据保护功能也可以加强信息的访问控制功能，使得企业内部更安全地进行信息共享和授权访问。可以指定信息只能被特定环境的授权人员访问，即使攻击者通过某种方式获得了密文信息或非法进入系统，也无法获知信息的真正内容。由此企业可以实现在安全有保证的前提下，利用信息网络的优势，降低运行成本，提高生产效率。

现有系统由于没有可信计算技术提供支持，系统管理者对网络系统的使用状况难以管理和控制，只能通过管理制度和手段来实现其对系统的管理目标。但是在一个更普遍的范围上看，一般企业没有、并且也难以对其日常业务实施类似的严格管理，致使系统使用方式和系统使命目标的背离，导致系统投入产出比和系统效率低下，更为严重的是，管理措施的缺位、技术措施的缺失所带来的系统滥用还很可能带来系统的安全问题。

企业信息系统的建设和使用目标必须服务于企业的业务使命。但现有的以计算机为主要业务操作平台的信息系统不能从技术上对系统拥有者和使用者加以分离，只能从管理制度上实现这一要求。企业作为系统拥有者，有权要求和规定使用者对其系统的使用方式和使用权限。但是由于管理力度和管理策略执行的不一致性，在很大范围内，系统滥用及其带来的安全问题是不可避免的。可信计算技术从技术上区分系统的拥有者和使用者，因此从这个意义上讲，可信计算技术对企业信息系统的信息安全和系统管理影响最为直接。

技术和管理是相互补充相互完善的，在技术发展水平或现状难以满足要求的时候，可以通过管理措施来加以弥补，但是技术的进步反过来又可以减少管理难度和管理成本，提高管理的效率和效果，可信计算技术就是对信息安全管理措施的补充和提高，通过可信计算技术，可以减轻非技术类管理措施的难度和压力，减少相关的冗余管理人员，提高信息安全管理的针对性，在节约生产成本的基础上增加企业产值。

因此，企业作为特殊的用户群体，在很大程度上具备可信计算技术应用的条件，如果能在技术成本等方面逐步降低门槛，应用前景十分乐观。

4．军队信息系统领域

军队信息系统的计算机网络规模庞大，终端和网络设备众多，应用环境复杂，军队信息系统中对数据安全和网络安全方面要求绝对保密，同时要求系统持续可靠运行。针对以上要求，以可信计算技术为基础，通过部署可信可控安全管理平台，采用嵌入密码型可信计算机、可信服务服务器、网络信任管理系统和智能IC卡，在保证节点可信安全的基础上，扩展到军队信息系统网络环境，可信可控安全管理平台对用户身份和操作平台进行识别和强制认证，对资源进行授权访问控制，对行为进行日志记录和责任审计，对接入网络和接出网络进行可信可控管理，对重要服务系统进行冗余备份，保证军队信息系统高速、安全、有序和畅通。

5.8.1　可信网络连接应用场景

随着计算机网络的逐渐发展，网络安全问题面临严峻的考验。目前业内的安全解决方案往往侧重于先防外后防内，先防服务设施后防终端设施。而可信计算则反其道而行之，首先保证所有终端的可信性，也即通过确保可信的组件来组建更大的可信系统。可信计算平台在底层进行更高级别防护，通过可信赖的硬件防止受到软件层次的攻击，可使用户获得更强的防护。

TNC是可信计算技术的一个重要组成部分。TNC的目的主要是将单个计算机系统可信状态扩展到计算机互联系统。根据今天的网络发展趋势看未来，有可能任何一个电子产品都可能会接入网络，而网络无处不在会导致攻击也无处不在。另外，不论在硬件、操作系统、网

络接入设备、应用系统都会存在漏洞，利用漏洞的恶意代码会攻击PC机、手机、数码照相机等等。为了确保终端和网络都是可信的，使得终端的可信扩展到网络，这就必须要求终端和接入控制器都是可信的。可信网络连接架构主要有以下的应用场景。

1．政府信息系统领域

近年来，我国在各级政府重要部门及岗位开始部署和实施电子政务系统，但目前电子政务系统主要存在以下安全问题：（1）计算机病毒层出不穷，直接影响电子政务的建设。（2）木马程序等间谍软件成为网络与信息安全保密的重要隐患。（3）黑客问题威胁电子政务系统的安全。可信网络连接架构主要从以下两方面解决上述问题：

对于政务内网，即政府部门内部的关键业务管理系统和核心数据应用系统，采用可信网络连接架构，使得内网用户在远程接入网络之前，需要进行用户的身份验证和终端平台的完整性评估，从而避免内部用户发起攻击，以及病毒、木马等恶意软件入侵内网系统，确保核心系统及数据的安全性、完整性和可用性。

对于政务外网，即政府部门内部以及部门之间的各类非公开应用系统所涉及的信息，采用可信网络连接架构，通过双向的身份验证及平台评估技术，保证了用户身份的合法性和终端的完整性，为各级政府部门网络管理员及用户之间的信息传递和共享提供了保障。双向的验证及评估技术确保了政务信息交互双方的利益和安全性，提高了整个政务系统的安全级别。

2．企业信息系统领域

企业网用户一般需要保证其网络安全、应用安全、数据安全、接入和可控接出管理。

可信网络连接架构能实现用户强制身份认证、终端身份认证，平台可信评估保证了网络的安全；可信度量、存储、报告、评估技术能防止恶意代码的侵入，保证了应用安全；TPM能实现与主CPU相隔离的对称、非对称加脱密运算，保证了数据安全；可信计算技术能实现用户身份、平台身份的认证，能细粒度地对用户和平台审计，保证接入和接出的可控。

3．电子商务领域

电子商务领域中，供应链是一个非常重要的组成部分。

供应链的目标是在企业之间交互传输动态的信息流和资金流，通过最终顾客的有效拉动，保证物流的有效、畅通。这个过程中，供应商、生产商、运输商和顾客之间都有信息的流动，该供应链能够有效畅通的一个前提是供应链中各个参与方都是诚实可信的。对于信息系统来说，各个参与方身份和平台应该是可信的，在每个参与方接入到该供应链系统时，都应对参与方的身份和平台进行认证和可信评估，只有符合安全策略的平台才允许接入该系统，这从根本上减少恶意情况的发生，保证信息流动的有效、畅通。

4．网上银行

随着信息化的不断发展，网上银行越来越得到广泛使用。网上银行已经推出了非常全面的业务，从账户查询、转账等这类日常生活的资金支付，到银证转账、外汇买卖等理财服务，都可以通过网上银行进行。但网上银行存在很多的安全隐患，如病毒、木马等。安全问题已经成为阻碍网上银行发展的一个重要问题。

通过可信网络连接架构，网上银行的系统在用户接入时，通过对用户的计算机平台状况进行度量和分析，如果平台安全状态不符合交易安全的要求，可以提醒用户停止交易，这样从根本上阻止了交易事故的发生。

银行帐户的操作存在交易者位置不确定的问题。例如客户的取款操作可能来自银行的柜台，也可能来自银行的ATM，仅仅通过用户身份鉴别即受理交易使得银行业务系统存在着安全隐患。应用可信计算技术，银行首先对客户进行身份鉴别，之后银行对交易执行终端的身份进行鉴别，这可以确定交易者的位置，从而提高银行防范交易风险的能力。

5．军事信息系统领域

军事环境下的网络对于网络连接的安全性和保密性要求很高。但军事环境下的网络更为复杂，数字化单兵、通讯车等移动终端和网络接入设备数量庞大、机动性强、网络拓扑结构变化频繁。现有军事网络连接方法只进行用户身份认证，而没有设备身份的认证，所以攻击者可以通过任意设备对网络进行攻击，安全性差。

可信网络连接架构在原有用户身份认证基础上，进行平台身份认证及平台完整性校验。在这一环境下，只有当攻击者拥有合法设备，并且获得设备使用权限的情况下，才可能进行攻击。也就是说，当攻击者采用非法设备进行攻击时，平台验证和平台完整性校验机制就可以检测出攻击，从而防止非法用户的连接。同时可以通过隔离修补机制，对接入设备进行管理，使得具有安全隐患的终端只能连接到受限的区域，增强网络的安全性。

本章小结

有别于传统信息安全技术，可信计算技术以“防内为主．内外兼防．狠抓终端源头安全”的模式，构筑全面高效的安全防护系统。

本章的内容包括以下方面：

（1）可信计算概述

讲述了可信计算的概念以及发展现状，给出了可信计算平台以密码技术为基础、以可信平台模块为信任根、以可信主板为平台、以可信基础支撑软件为核心、以可信网络连接为纽带的体系结构。

（2）可信计算平台密码方案

密码技术是可信计算平台的基础，为可信计算平台实现其安全功能提供密码支持。可信计算密码支撑平台中配备的密码算法包括：随机数产生算法、杂凑算法、消息验证码算法、对称密码算法和公钥密码算法。可信计算平台对密码的使用涉及到密钥迁移、授权协议、DAA 数字签名等。根据密钥的使用范围，平台中的密钥可以分为三类：平台身份类密钥、平台存储类密钥、用户类密钥。密码模块密钥、存储主密钥、平台所有者的授权数据直接存放在可信密码模块内部，通过可信密码模块的物理安全措施保护；平台身份密钥、平台加密密钥、用户密钥等可以加密保存在模块外部。平台通过设置密钥实体的权限数据来控制用户对密钥的访问。权限数据必须被加密存储保护。平台设置密码模块证书和平台证书两种数字证书。平台证书采用“双证书”机制，平台证书包含平台身份证书和平台加密证书，平台身份证书用于平台身份的证明，平台加密证书执行加密运算，用于平台间密钥迁移以及其它敏感数据的交换保护。

（3）可信平台控制模块

可信平台控制模块是可信应用的核心控制模块，它为可信应用提供物理上的三个根功能：可信度量根、可信报告根与可信存储根。以可信平台控制模块为基础，可以扩展出可信计算平台的可信度量功能、可信报告功能与可信存储功能。在 TPCM 内部应包括如下单元：微处理器、非易失性存储单元、易失性存储单元、随机数发生器、密码算法引擎、密钥生成器、定时器、输入输出桥接单元和各种输入输出控制器模块。可信平台模块实现了可信度量、可信存储和可信报告三大基本功能，实现可信平台用户管理、可信平台控制模块内部固件和可信平台控制模块内部维护管理三个辅助功能。

（4）可信平台主板

可信平台控制模块安装在可信主板上。可信主板构成了可信计算的舞台。可信计算主板涉及的功能主要包括信任链的建立，附加有可信安全硬盘存储等功能。可信链的建立基于可信度量，可信度量的方法是代码的完整性度量。完整性度量功能检查运行前后软硬件代码的一致性，从而保证代码不被外部篡改。

可信计算平台主板是由TPCM和其它通用部件组成，以TPCM自主可信根（RT）为核心部件实现完整性度量和存储机制，并实现平台可信引导功能。

（5）可信基础支撑软件

可信基础支撑软件由可信软件基TSB、可信基础支撑软件系统服务TSS和可信基础支撑软件应用服务TAS三个部分组成，向可信计算平台上层应用提供完整性、数据保密性和身份认证管理功能的标准接口，其基本功能是提供完整性管理、数据保密性管理和身份认证管理功能。

（6）可信网络连接

可信网络连接架构中，存在三个实体：访问请求者、访问控制器和策略管理器，从上至下分为三个层次：完整性度量层、可信平台评估层和网络访问控制层。它通过访问请求者、访问控制器以及策略管理器三个实体来实现访问请求、访问控制以及策略管理的功能。

（7）可信计算应用

本章最后主要从可信计算平台以及可信网络连接两个方面介绍了可信计算技术的在不同领域里的应用场景。

习题

1．如何理解可信计算的概念，可信计算和传统的信息安全保护机制的不同点是什么？
2．概述可信计算平台的体系结构和主要功能。
3．描述密码算法与可信密码支撑平台的关系。
4．概述可信平台控制模块的三大功能。
5．描述信任链建立过程。
6．概述可信基础支撑软件的三个层次。
7．概述可信网络连接架构中三个实体完成的主要功能。
8．举例说明可信计算的应用。

第 6 章　信息安全等级保护

本章要点

- 第三级、第四级系统安全设计技术要求
- 一个第三级应用支撑平台的设计实例

6.1　信息安全等级保护综述

信息安全等级保护是我国信息安全保障工作的纲领性文件(《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号）提出的工作任务，是我国一项重要的信息安全保障工作。其基本原理是，不同的信息系统有不同的重要性，在决定信息安全保护措施时，必须综合平衡安全成本和风险。因此，从加强信息系统安全监管的角度，国家需要对不同等级的系统提出不同的安全要求。

6.1.1　等级保护的原则

信息系统安全等级保护是指，国家对涉及国家安全和社会稳定与安全，公民、法人和其他组织的合法权益的信息系统，按其重要程度和实际安全需求，分级、分类、纵深采取保护措施，保障信息系统安全正常运行和信息安全。特别是要对基础信息网络和重要信息系统按其重要程度和实际安全需求，分级进行保护，分类指导开展安全等级保护，分小区（局域）纵深多级防护，分阶段推进安全等级保护工作，提高国家信息安全综合防护能力，进而保障国家安全，维护信息社会秩序和稳定，促进经济发展，提高综合国力。

信息安全等级保护的核心是对信息安全分等级、按标准进行建设、管理和监督。信息安全等级保护制度遵循以下基本原则：

1）明确责任，共同保护。通过等级保护，组织和动员国家、法人和其他组织、公民共同参与信息安全保护工作；各方主体按照规范和标准分别承担相应的、明确具体的信息安全保护责任。

2）依照标准，自行保护。国家运用强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行定级、自行保护。

3）同步建设，动态调整。信息系统在新建、改建、扩建时应当同步建设信息安全设施，保障信息安全与信息化建设相适应。因信息和信息系统的应用类型、范围等条件的变化及其它原因，安全保护等级需要变更的，应当根据等级保护的管理规范和技术标准的要求，重新确定信息系统的安全保护等级。等级保护的管理规范和技术标准应按照等级保护工作开展的实际情况适时修订。

4）指导监督，重点保护。国家指定信息安全监管职能部门通过备案、指导、检查、督促整改等方式，对重要信息和信息系统的信息安全保护工作进行指导监督。国家重点保护涉及国家安全、经济命脉、社会稳定的基础信息网络和重要信息系统，主要包括：国家事务处理信息系统（党政机关办公系统）；财政、金融、税务、海关、审计、工商、社会保障、能源、交通运输、国防工业等关系到国计民生的信息系统；教育、国家科研等单位的信息系统；公用通信、广播电视传输等基础信息网络中的信息系统；网络管理中心、重要网站中的重要信息系统和其它领域的重要信息系统。

等级保护是一个灵活的概念，它并非硬性的规定，而是一些原则性的指导思想。等级保护与现有系统的建设也并没有本质的冲突。实行信息安全等级保护，应当以等级保护的方法对现有系统进行加固改造，保障安全的互联互通和信息共享，保障现有系统安全，使现有系统活起来，发挥现有系统在电子政务和电子商务方面的作用，而不是弃之不用或推倒重来。建设过程中，要把握以下几个重要原则：坚持一手抓发展，一手抓安全；坚持以改革开放求安全；坚持管理与技术并重，坚持统筹兼顾，突出重点。

6.1.2 等级划分

为了进一步提高信息安全的保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，1994年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定，“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。2003年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）明确指出，“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南”。

等级保护是针对我国关系到国计民生的各类信息系统进行分级分类，对不同级别、类别的系统实施重点、适度的保护。各类系统的社会和经济价值保护需求不同，系统中信息的敏感性不同，信息系统所属部门、单位的重要性不同，应用的性质不同，它们的安全需求以及安全建设成本也因此必然有所差异，必须这些系统进行分级分类，实行等级保护。

2007 年 6 月，公安部等四部门联合发布了《信息安全等级保护管理办法》，该办法规定，根据信息系统在国家安全、经济建设、社会生活中的重要程度，其遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，其安全保护等级由低到高划分为五级。

- 第一级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
- 第二级：信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
- 第三级：信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。
- 第四级：信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
- 第五级：信息系统受到破坏后，会对国家安全造成特别严重损害。

表 6-1 给出了安全等级的定级原则。

表 6-1　安全等级定级原则

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

第四、第五级的信息系统是国家的核心信息系统，是国家政治安全、疆土安全和经济安全之所系。

信息系统的安全等级保护应根据信息系统安全定级情况来确保信息系统具有相应等级的基本安全保护能力，不同安全等级的信息系统要求具有不同的安全保护能力，即第一级信息系统应该具有与第一级安全保护要求相符的能力、第二级信息系统应该具有与第二级安全保护要求相符的能力，以此类推。显然，信息系统的安全等级越高，其安全要求也就越高。

不同安全等级的信息系统应该具备的基本安全保护能力描述如下：

- 第一级安全保护能力：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其它相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。
- 第二级安全保护能力：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其它相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全相关事件，在系统遭到损害后，能够在一段时间内恢复部分功能。
- 第三级安全保护能力：应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其它相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全相关事件，在系统遭到损害后，能够较

快恢复绝大部分功能。

- 第四级安全保护能力：应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾难、以及其它相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全相关事件，在系统遭到损害后，能够迅速恢复所有功能。
- 第五级安全保护能力：简单地说，是在第四级的安全保护能力的基础上，由访问控制监视器实行访问验证，采用形式化技术验证相应的安全保护能力确实得到实现。

6.1.3 等级保护相关法规标准

国家已针对等级保护提出了一系列的法规标准，是各单位建设等级保护系统的依据，可分为政策法规和技术性法规标准两类。

政策法规为等级保护提供管理方面的依据。最早提及等级保护的法规是 1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》。中办发的 2003 27 号文件《国家信息化领导小组关于加强信息安全保障工作的意见》对等级保护提出了更明确的工作要求。2004 年出台的《关于信息安全等级保护工作的实施意见》进一步明确了信息安全等级保护制度的基本内容：

- 根据信息和信息系统在国家安全、社会秩序、公共利益、社会生活中的重要程度；遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；针对信息的保密性、完整性和可用性要求及信息系统必须要达到的基本的安全保护水平等因素，确定信息和信息系统的安全保护等级，共分五级。
- 国家通过制定统一的管理规范和技术标准，组织行政机关、公民、法人和其他组织根据信息和信息系统的不同重要程度开展有针对性的保护工作。国家对不同安全保护级别的信息和信息系统实行不同强度的监管政策。
- 国家对信息安全产品的使用实行分等级管理。
- 四是信息安全事件实行分等级响应、处置的制度。

2006 年 3 月，国家《信息安全等级保护管理办法》开始正式实施。《信息安全等级保护管理办法》给出了国内信息系统级别划分的原则，另外还从安全管理、保密管理、密码管理、法律责任等方面作了具体规定。

技术性标准以 GB 17859-1999《计算机信息系统安全保护等级划分准则》作为基础。该标准采取了宜原则不宜细的制定方法，目的是为安全产品的开发、具体标准的制定、安全系统的建设与管理、相关法律法规及其执法的提供技术指导和基础。

GB 17859-1999 发布后，我国还从技术和管理方面，对信息系统以及安全产品的评估提出了具体的标准。在等级保护的标准体系中，除了面向评估者的标准外，还需要有面向等级保护建设者的标准，来指导建设者部署符合等级保护要求的安全防护措施。目前，这方面的标准主要有两个：GB/T 22239-2008《信息系统安全等级保护基本要求》（以下简称《基本要求》）以及《信息系统等级保护安全设计技术要求（报批稿）》（以下简称《技术要求》），其中，《基本要求》偏重于硬件环境和管理，《技术要求》则偏重于等级保护的技术实现。

《基本要求》根据现有技术的发展水平，提出和规定了不同安全等级信息系统的最低保护要求，即基本安全要求，基本安全要求包括基本技术要求和基本管理要求两大类。

技术类安全要求与信息系统提供的技术安全机制有关，主要通过在信息系统中部署软硬件并正确地配置其安全功能来实现；管理类安全要求与信息系统中各种角色参与的活动有关，主要通过控制各种角色的活动，从政策、制度、规范、流程以及记录等方面做出规定来实现。

基本技术要求一般从物理安全、网络安全、主机安全、应用安全和数据安全等五个方面考虑。

基本管理要求一般从安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等五个方面考虑。

《技术要求》则以访问控制为核心，从技术上规范了信息系统等级保护安全设计要求。本章第二节重点描述技术要求中的具体内容。

6.2 等级保护安全设计技术要求

6.2.1 等级保护安全设计技术框架

定级系统的安全保护环境是由一个中心、三层纵深防御体系构成的单一级别安全保护环境及其互联构成的。一个中心是指安全管理中心，三层纵深防御体系则由安全计算环境、安全区域边界以及安全通信网络组成。

安全计算环境是对定级系统的信息存储与处理进行安全保护的部件。计算环境由定级系统中完成信息存储与处理的计算机系统硬件和系统软件以及外部设备及其联接部件组成，也可以是单一的计算机系统。安全计算环境按照保护能力可划分为第一级安全计算环境、第二级安全计算环境、第三级安全计算环境、第四级安全计算环境和第五级安全计算环境。

安全区域边界是对定级系统的安全计算环境的边界，以及安全计算环境与安全通信网络之间实现连接功能进行安全保护的部件。安全保护主要是指对安全计算环境以及进出安全计算环境的信息进行保护。安全区域边界按照保护能力可划分为第一级安全区域边界、第二级安全区域边界、第三级安全区域边界、第四级安全区域边界和第五级安全区域边界。

安全通信网络是对定级系统安全计算环境之间进行信息传输实施安全保护的部件。安全通信网络按照保护能力可划分第一级安全通信网络、第二级安全通信网络、第三级安全通信网络、第四级安全通信网络和第五级安全通信网络。

安全管理中心对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台。第二级及第二级以上的系统安全保护环境通常需要设置安全管理中心，分别称为第二级安全管理中心、第三级安全管理中心、第四级安全管理中心和第五级安全管理中心。

信息系统等级保护安全技术设计包括各级系统安全保护环境的设计及其安全互联的设计，如图 6-1 所示。各级系统安全保护环境由相应级别的安全计算环境、安全区域边界、安全通信网络和（或）安全管理中心组成。定级系统安全互联由安全互联部件和跨系统安全管理中心组成。

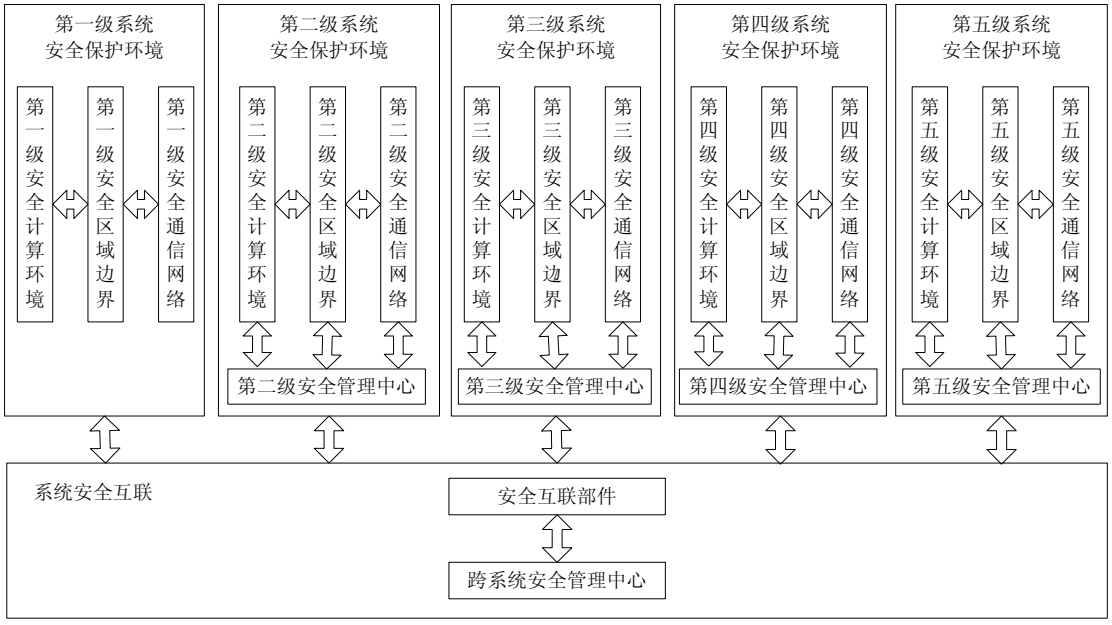


图 6-1 信息系统等级保护安全技术设计内容

不同级别的等级保护安全技术之间存在着层层嵌套的关系，从第一级开始，每一级在继承其低一级别所有安全要求的基础上，增补一些安全要求，或对上一级别的特定安全要求有所加强。每一级都有自己的安全防护目标以及对应的关键技术。

等级保护安全技术要求在可信计算基（TCB）上实现。可信计算基作为计算机系统信息安全的基础，其自身需要有一定的安全强度。特别是在高安全级别信息系统环境中，对可信计算基的强度有具体的规定。一般而言，系统的安全机制作为可信计算基的一部分，应考虑在操作系统层面实现，以防

止安全机制被旁路。

6.2.2 第一级信息系统的安全

第一级系统为用户自主保护级，其核心技术为自主访问控制。其设计目标是：落实 GB 17859-1999 对第一级系统的安全保护要求，实现定级系统的自主访问控制，使系统用户对其所属客体具有自我保护的能力。

第一级安全系统在计算环境上的主要技术要求包括：采用采用一般性的口令鉴别机制进行的用户鉴别以及对口令数据进行保护；主体粒度为用户/用户组，客体粒度为文件和数据库表的自主访问控制机制；采用常规校验方法的用户数据完整性保护机制，以及恶意代码防范软件。

第一级安全区域边界的主要技术要求则包括使用区域边界包过滤技术，根据区域边界安全控制策略，由数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包通过该区域边界。以及使用恶意代码防范措施，在安全区域边界设置防恶意代码软件，并定期进行升级和更新，以防止恶意代码入侵。

第一级的安全通信网络设计技术要求则要求采用各种常规校验机制，检验网络传输数据的完整性，并能发现其完整性被破坏的情况。

6.2.3 第二级信息系统的安全

第二级的关键技术为审计。与第一级——用户自主保护级相比，本级的信息系统TCB实施一个粒度更细的自主访问控制，并通过登录规程、审计安全相关事件和隔离资源，提供对用户行为追溯的能力。

第二级要求TCB定义和控制系统内命名用户对命名客体的访问。实施机制（例如访问控制表）应该允许用户以命名个体身份和（或）用户组身份指定和控制对那些客体的共享，应该防止未授权用户读取敏感信息，而且应该限制访问权限的扩散。

自主访问控制机制应该根据用户指定方式或默认方式来防止对客体的非授权访问。访问控制的粒度要细到单个用户。没有存取权的用户只允许由授权用户分配对客体的访问权。

第二级信息系统的TCB应该能创建和维护对受保护客体的访问审计轨迹，并能防止未授权用户对它进行修改或破坏。对审计数据的读取只限于那些被授权的用户。对不能由TCB独立分辨的审计事件，审计机制应该提供审计记录接口，可由授权主体调用。这些审计记录区别于TCB独立分辨的审计记录。

TCB 应该能记录下述事件：使用身份标识与鉴别机制；将客体导入用户地址空间（例如，打开文件、程序初始化）；删除客体；由操作员、系统管理员和（或）安全管理员实施的动作；以及其它安全相关事件。对于每一事件，其审计记录应清晰包括：事件的日期与时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录应该包含请求的起源（例如，终端标识符）。对于客体导入用户地址空间事件和客体删除事件，审计记录应该包含客体名称。系统管理员应该能够选择性地审计任意一个或多个标识用户的行为。

第二级要求的是更强的自主安全保护能力，而安全系统的审计功能可以看作是对自主访问控制机制的加强。第一级中对使用者执行非法授权行为是没有任何制约的。第二级安全系统则可以通过安全审计机制，对用户的非法授权行为提供记录证据，以备日后追查。这对于内部恶意用户是一个有效的威慑。

另外，第二级安全系统还要求防范客体重用的功能，要求对 TCB 空闲存储客体池中的一个客体进行初始指派、分配或再分配一个主体之前，应撤消对该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，该主体不能获得原主体活动所产生的任何信息，包括加密信息。这也可以看作是对自主访问控制的加强。

二级安全系统在区域边界上，要求具备区域边界协议过滤功能，能根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。同时，要求在安全区域边界设置必要的审计机制、防恶意代码网关以及边界探测软件，由安全管理中心管理。

二级安全系统在通信网络上，则需要具备网络安全审计、网络数据传输完整性保护以及网络数据传输保密性保护等安全要求。

二级系统要求集中式的管理中心，该管理中心的系统管理和审计管理需要相互独立，系统管理可

通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份和授权管理、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复以及恶意代码防范等。系统管理员应进行严格的身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。而审计管理可通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。安全审计员应进行严格的身份鉴别，并只允许其通过特定的命令或操作界面进行安全审计操作

6.2.4 第三级信息系统的安全

我们把三级及以上要求的信息系统统称为高安全级别信息系系统。高安全级别信息系统在安全功能上要求以强制访问控制为核心。安全系统需保持系统中主、客体安全标记的完整性，并使用其实现一组强制访问控制规则。信息系统必须给主要的数据结构分配敏感标记。系统开发者也应提供构建TCB的安全策略模型和关于TCB的规范说明。

强制访问控制是三级安全系统的关键技术，也是高安全级别信息系统安全功能上的核心内容，部署了强制访问控制机制的系统，即使是合法用户，也不能违反强制访问控制的规则。部署强制访问控制机制的信息系统，其安全保护的特点与我们通常概念上的安全有较大区别。高安全级别信息系统的防护重点是内部，其对病毒、黑客的防护是通过增强系统自身对恶意代码的免疫能力来实现的，而不依赖于传统的防病毒、防火墙、入侵检测等技术。高安全级别信息系统并不一定要求系统中所有子系统都是相应级别的，但其TCB的构建必须依托对应级别的安全操作系统。

1．第三级安全的特点

本级的 TCB 具有系统审计保护级的所有功能。此外，还需提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述。具有准确地标记输出信息的能力。消除通过测试发现的任何缺陷。

三级系统的 TCB 应维护与主体及其控制的存储客体（例如，进程、文件、段、设备）相关的敏感标记。这些标记应该当作强制访问决策的基础来使用。敏感标记应该准确地体现与其相关的指定主体或客体的安全级别。当敏感标记被 TCB 输出时，它们应该准确而无歧义地代表内部标记，并且应该与正待输出的信息关联起来。

在对安全管理员进行严格的身份鉴别和权限控制基础上，由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制；强制访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级；应确保系统安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。第三级信息系统的强制访问控制规则不仅在安全计算环境上部署，也需要在安全边界上实施。

在安全管理上，第三级安全系统需要遵循系统管理员、安全管理员和审计管理员三权分立的要求。

系统管理应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和（或）异地灾难备份与恢复等。安全管理应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置统一的安全策略。审计管理应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。应对审计记录进行分析，并根据分析结果进行处理。

系统管理员、安全管理员和审计管理员均应进行严格的身份鉴别，只允许其通过特定的命令或操作界面进行系统管理、安全管理和安全审计操作。另外，系统用户的操作权限同样也需要和三种管理员的权限分离开来。

2．高安全级别操作系统黑客、病毒免疫的机理

一个安全策略配置良好的高安全级别信息系统，应当是对黑客、病毒具有免疫能力，不需要使用防病毒、防火墙或入侵检测等技术。对于四级以上的高安全级别信息系统，防火墙、防病毒软件、入侵检测以及系统补丁程序等不但不会起到保护作用，反而可能成为安全的威胁。

考虑病毒的传播机理，病毒实际上是通过系统漏洞，获取了系统特权，并利用这些特权来非法复制自身，并将自己传播到系统的其它机器之中。无论是引导区病毒、执行程序病毒还是宏病毒，其传播和发作的前提都是能够获取特权以及能够非法复制自身。而在部署强制访问控制机制的系统中，不存在通常意义上的超级用户特权，对系统文件的所有修改必须由系统管理员经过严格的身份认证后，使用特定的工具来实现。而系统管理员的安装环境可以通过严格的策略设置和完整性检验来确保其“干净”。病毒无法获取系统管理员的权限，也就无法进行传播。

对黑客的免疫机理与对病毒的防护机理类似，以黑客们经常利用的缓冲区溢出攻击为例。高安全级别信息系统并不能保证应用中不存在缓冲区溢出的攻击漏洞，但是，即使系统中存在的缓冲区溢出漏洞被黑客发现且利用，成功地执行了黑客传入的恶意代码，黑客也只是获取了以当前用户身份执行程序的权限，而这一权限并不给黑客提供违反强制访问控制策略的权限。例如，应用在高保密级别的环境下运行，接收低保密级别的信息输入，这是满足BLP模型的，即使黑客从低保密级别环境中通过缓冲区溢出漏洞，成功地使应用运行黑客注入的代码，并让这些代码向黑客发送涉密信息，由于BLP模型不可下写的限制，涉密信息仍然不会被发送给黑客，也就不会造成泄密事件。

但是，如果系统中运行着防病毒、入侵检测、自动补丁程序等软件，他们需要对系统进行检查和修改的特权，这些特权将绕过强制访问控制机制，成为系统的安全后门，如果被攻击者利用，就将成为系统的安全威胁。因此，高安全级别信息系统的安全重点应放在安全策略的合理配备上，而不能依赖防火墙、防病毒产品、入侵检测系统、系统补丁等目前市面上流行的安全产品和安全解决方案。

6.2.5 第四级信息系统的安全

信息系统的第四级安全是结构化保护级。这一级的安全功能要求与第三级基本相同，但在安全保障上有所加强，要求通过结构化的保护措施，有效加强系统TCB的抗攻击能力，达到防止系统内部具有一定特权的编程高手攻击的能力。

四级安全信息系统的TCB要求建立于一个明确定义的和有文档说明的形式化安全策略模型之上，该模型要求将第三级系统中的自主和强制访问控制扩展到系统的所有主体与客体。此外，还要考虑隐蔽通道。本级的TCB必须被结构化为关键保护元素和非关键保护元素。TCB接口也必须被清楚定义，TCB设计与实现应使其易于经受更充分的测试和更完全的复审。加强了身份鉴别机制；为支持系统管理员和操作员的职能，提供可信工具包管理；增加了严格的配置管理控制。系统具有相当的抗穿透能力。

四级安全信息系统的TCB应该为自身的运行维持一个域，该域能防止外部的干扰或篡改（例如，通过对其代码或数据结构的修改）。TCB应该隔离受保护的资源，以便它们服从于访问控制和审计要求。TCB应该通过其监管的不同地址空间来维护进程隔离。

TCB在内部应该被结构化为良好定义的、尽可能独立的模块，它应该有效地使用可获得的硬件资源来区分关键保护元素和非关键保护元素。TCB模块应该被设计为满足最小特权原则被实施。硬件方面的特性（例如，分段）应该被用来支持逻辑上不同的具有可读或可写属性的存储客体。TCB的用户接口应该完全被定义，且TCB的所有元素应该能够被识别。

在《设计要求》中，对安全信息系统的结构化保护提出了三个方面的要求，分别是安全保护部件结构化设计技术要求、安全保护部件互联结构化设计技术要求以及重要参数结构化设计技术要求。

安全保护部件结构化设计技术要求第四级系统安全保护环境各安全保护部件的设计应基于形式化的安全策略模型。安全保护部件应划分为关键安全保护部件和非关键安全保护部件，并防止敏感信息危害安全策略地从关键安全保护部件流向非关键安全保护部件。关键安全保护部件应划分功能层次，并明确定义功能层次间的调用接口，确保接口之间的信息安全交换。

安全保护部件互联结构化设计技术要求第四级系统各安全保护部件之间互联的接口功能及其调用关系应明确定义；各安全保护部件之间互联时，需要通过可信验证机制相互验证对方的可信性，确保安全保护部件间的可信连接。

重要参数结构化设计技术要求应对第四级系统安全保护环境设计实现的与安全策略相关的重要数据结构给出明确定义，包括参数的类型、使用描述以及功能说明等，并用可信验证机制确保数据不被篡改。

在实际工程开发中，对于信息系统的结构化保护，可以采用“TCB 扩展”的系统“结构化保护”方案，该方案的主要技术思想是：

- 建立一个足够小的、能够通过形式化方法加以定义和描述的系统初始 TCB；
- 基于系统初始 TCB，通过可以被证明的信任传递过程实现可信的计算平台，并保证单计算平台 TCB 是可以形式化定义和描述的；
- 基于可信的计算平台，通过身份认证和平台可信证明等机制，建立可信的应用区域，实现可信的应用区域边界保护，保证应用区域 TCB 是可以形式化定义和描述的；
- 基于可信的应用区域和其边界，通过可信的网络连接，实现可信的系统，保证系统 TCB 是可以形式化定义和描述的；
- 基于可信管理，实现系统的最小特权。

通过上述 TCB 扩展过程，可以实现一个满足图 6-1、6-2 和 6-3 技术保障结构的第四级安全的信息系统。

基于 TCB 扩展的系统“结构化保护”保证方案有以下好处：将大规模复杂系统中难以对 TCB 进行形式化定义和描述的问题转化为两个相对简单的相对容易解决的问题，即对一个足够小的系统初始 TCB 的形式化定义和描述以及对信任传递和平台可信证明过程的描述。

为此，基于 TCB 扩展的系统“结构化保护”要解决以下两个问题：

- 系统初始化 TCB 的选择，该 TCB 的选择应该足够小、并且易于形式化定义和描述；
- TCB 扩展过程的可证明性。

可信计算技术为上述问题的解决提供了理论和实践的可能。以可信计算技术为基础，可以选择包括可信硬件和系统启动可信软件在内的可信根作为系统初始化 TCB。该可信根完全能够满足“足够小、并且易于形式化定义和描述”的要求；从该可信根出发，通过信任传递、可信证明等过程实现 TCB 的扩展，最终实现可信的信息系统。可信计算技术相关领域的研究显示，信任传递、可信证明等 TCB 扩展机制完全是可以实现的。

在可信计算技术支持下，基于 TCB 扩展的系统“结构化保护”保障过程可以通过图 6-2、6-3 和 6-4 表示。

首先，是单个计算平台上的 TCB，它是足够小的，见图 6-2。

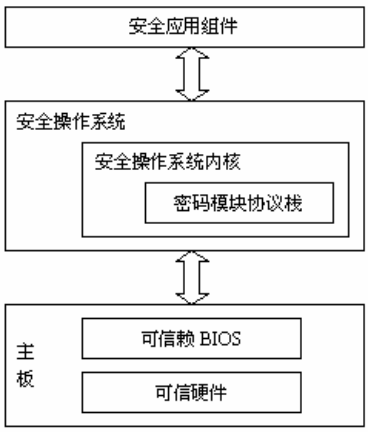


图 6-2　基于可信根和信任传递的计算平台“结构化保护”

其次，TCB 从单个计算平台扩展到应用区域，见图 6-3。

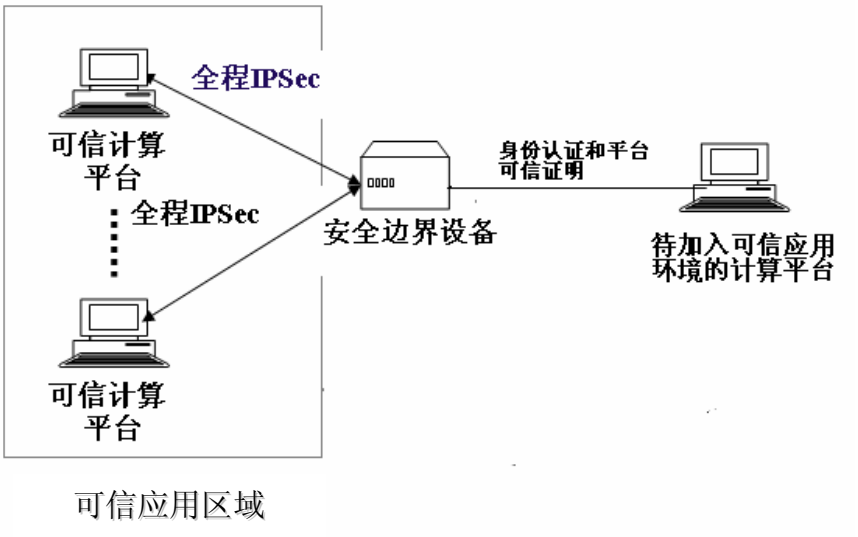


图 6-3　基于可信计算平台和平台证明机制的应用区域“结构化保护”

最后，TCB 从应用区域扩展到网络环境下的信息系统，见图 6-4。

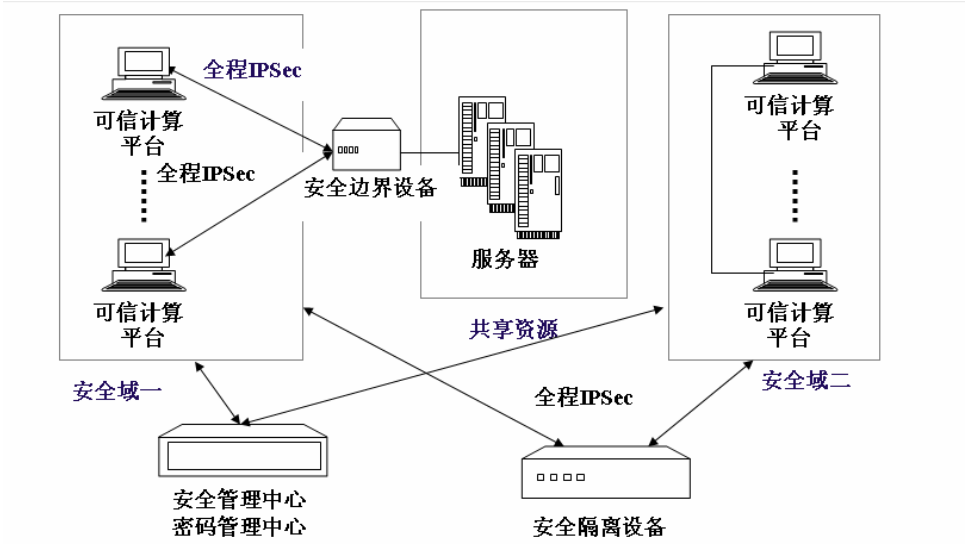


图 6-4　基于可信网络连接的信息系统“结构化保护”

6.2.6　第五级信息系统的安全

信息系统的第五级安全是访问验证保护级。其关键技术为访问监控器，要求基于形式化验证技术，在第四级系统安全保护环境的基础上，实现访问监控器，仲裁主体对客体的访问。并支持安全管理职能，审计机制可根据审计记录及时分析发现安全事件并进行报警，提供系统恢复机制，从而使系统具有很强的抗渗透能力。

五级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小程度。支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统具有很高的抗渗透能力。

五级系统在安全功能方面与四级相比，增加了实时监控的功能以及可信恢复的功能。在安全保证机制上，五级系统可信计算基满足抗篡改、足够小，能够分析和测试三项要求，要以形式化验证的方法确认系统TCB部分的不可旁路、不可篡改。

五级信息系统的要求形式化验证，下面对形式化的一些概念作简单的介绍。

1．形式化证明　Formal Proof

一个完整的和令人信服的数学论证，为每一个证明步骤、为每个定理或一组定理的真实性呈现了完全的逻辑合理性。

形式化验证过程使用形式化证明方法显示形式化说明书中某些性质的真实性，并且为证明计算机程序满足它们的设计规格说明提供基础。

2．形式化安全策略模型　Formal Security Policy Model

安全策略的一种数学上精确的陈述。为了是足够精确的，这样的模型必须描述系统的初始状态、系统从一个状态到另一个状态的演进方式、以及系统安全状态的一个定义。

为了作为TCB的一个基础而被接受，模型必须被形式化证明所支持，即如果系统的初始状态满足安全状态的定义，且如果所有的被模型要求的假设皆成立，那么，系统所有的未来状态都将是安全的。

一些形式化建模技术包括：状态跃迁模型、时序逻辑模型、符号语义模型、代数规格模型等。

3．形式化顶层说明书　Formal Top-Level Specification　（FTLS）

一个用形式数学语言书写的系统设计说明书。采用它是为了允许定理被假设和被形式化证明，这些定理将表明系统设计规格与其形式化需求规格之间的一致性。

有时，FTLS也被称为形式化设计说明书，或形式化设计规范。

4．形式化验证　Formal Verification

为用证据表明两个不同层次的系统说明书之间的一致性（或对应性），使用形式化方法证明其的过程。

如果证明的是系统形式化设计说明书与包含于需求说明书中的形式化安全策略模型之间的一致性，则该过程被称为设计验证（Design Verification）。

如果证明的是形式化设计说明书与产品实现之间的一致性，则该过程被称为实现验证（Implementation Verification）。根据实现内容的不同，实现验证又可以分为代码验证、固件验证和硬件验证。

形式化验证技术起源于20世纪60年代的软件危机时期，采用定理证明、模型检验、等价性检验等方式。典型的定理证明工具有高阶逻辑定理证明器（Higher Order Logic，HOL）、原型验证系统（Prototype Verification System，PVS）等，模型检验工具有符号模型验证器（Symbolic Model VerifIer，SMV）、定界模型检验技术等。

HOL通过元语言ML（Meta-Language）与用户交互，由用户选择推理规则，HOL应用这些规则。PVS基于一阶逻辑，主要包括规格说明语言和证明检验器。SMV基于控制树逻辑，主要包括程序语言和证明理论。

定理证明的过程是：首先从需求分析中抽取系统的模型，表示成形式逻辑的命题、谓词、定理、推理规则等，需要验证的性质被表示成定理的形式。定理证明的过程就是在验证者的引导下，不断地对公理、已证明的定理施加推理规则，产生新的定理，直至推导出所需要的定理。

典型的定理证明系统如HOL、PVS等都内置各种推理规则、推理对策、元对策等，由验证者决定推理方向。定理证明的验证方法需要具有良好数学训练和经验的验证者来引导推理进程。各个定理证明系统需要的交互程度不同：HOL需要更详细的引导，提供更强的灵活性，而PVS则更自动化，但灵活性差一些。

形式化代码验证也就是我们常说的程序正确性证明，在目前尚难以有效做到，因此，常用的替代方法是软件测试或其它非形式化技术。

6.3　定级系统安全保护环境主要产品类型及功能

不同级别的安全信息系统，需要选择相应的安全产品来实现等级保护安全机制。第一级、第二级安全系统的安全保护可以通过市场上流行的安全产品合理配置来实施，而第三级以上的高安全级别信息系统则必须基于安全操作系统，在对信息系统内部工作流程进行合理的安全分析和标识的基础上进行。

下面列出各级安全保护环境可选的主要产品类型和该产品的功能。注意，这些产品在安全保护环境中的使用并不是独立的，而必须按照保护环境的安全要求，合理配置，综合使用，最终实现对系统的整体安全解决方案。

6.3.1 第一级系统安全保护环境主要产品类型及功能

第一级系统安全保护环境中，应按照第一级系统安全保护环境的设计目标和设计策略，落实第一级安全计算环境、安全区域边界和安全通信网络的设计技术要求，选择符合相应要求的安全产品进行集成。表 6-1 是第一级系统安全保护环境集成中各部分的安全功能及可供参考的主要产品类型。

表 6-1 第一级系统安全保护环境主要产品类型及功能

使用范围	安全功能	产品类型
安全计算环境	用户身份鉴别	操作系统、数据库管理系统等
	自主访问控制	
	用户数据完整性保护	
	恶意代码防范	主机防病毒软件*等
安全区域边界	区域边界包过滤	防火墙、网关等
	区域边界恶意代码防范	防病毒网关*等
安全通信网络	网络数据传输完整性保护	路由器等
注：其中带“*”的项表示其设备的功能可在信息系统安全设计技术方案中统一考虑。		

6.3.2 第二级系统安全保护环境主要产品类型及功能

第二级系统安全保护环境中，应按照第二级系统安全保护环境的设计目标和设计策略，落实第二级安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计技术要求，选择符合相应要求的安全产品进行集成。此外，系统安全集成还可包括通过设置数据和设备的备份与恢复机制，支持用户和系统管理员对被破坏或丢失的数据进行恢复，以及在设备和系统出现故障时进行恢复。表 6-2 是第二级系统安全保护环境集成中各部分的安全功能及可供参考的主要产品类型。

表 6-2 第二级系统安全保护环境主要产品类型及功能

使用范围	安全功能	产品类型
安全计算环境	用户身份鉴别	操作系统、数据库管理系统、安全审计系统*、身份鉴别系统等
	自主访问控制	
	系统安全审计	
	用户数据完整性保护	
	用户数据保密性保护	
	客体安全重用	
	恶意代码防范	主机防病毒软件*等
安全区域边界	区域边界协议过滤	防火墙、网关等
	区域边界安全审计	
	区域边界恶意代码防范	防病毒网关*等
	区域边界完整性保护	防非授权外联系统、入侵检测系统等
安全通信网络	网络安全审计	VPN、加密机*、路由器等
	网络数据传输完整性保护	
	网络数据传输保密性保护	
安全管理中心	系统管理	安全管理平台
	审计管理	
注：其中带“*”的项表示其设备的功能可在信息系统安全设计技术方案中统一考虑。		

6.3.3 第三级系统安全保护环境主要产品类型及功能

第三级系统安全保护环境中，应按照第三级系统安全保护环境的设计目标和设计策略，落实第三级安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计技术要求，选择符合相应要求的安全产品进行集成。此外，系统安全集成还应包括通过设置数据和设备的备份与恢复机制，支持用户和系统管理员对被破坏或丢失的数据进行恢复，以及在设备和系统出现故障时进行恢复；根据应用对业务连续性的要求，设置系统级灾难备份与恢复机制，并支持应急处理。表 6-3 是第三级系统安全保护环境集成中各部分的安全功能及可供参考的主要产品类型。

表 6-3 第三级系统安全保护环境主要产品类型及功能

使用范围	安全功能	产品类型
安全计算环境	用户身份鉴别	操作系统、数据库管理系统、安全审计系统*、终端安全管理*、身份鉴别系统等
	自主访问控制	
	标记与强制访问控制	
	系统安全审计	
	用户数据完整性保护	

	用户数据保密性保护	
	客体安全重用	
	系统可执行程序保护	操作系统等
安全区域边界	区域边界访问控制	安全隔离与信息交换系统、安全网关等
	区域边界协议过滤	
	区域边界安全审计	
	区域边界完整性保护	
安全通信网络	网络安全审计	VPN、加密机*、路由器等
	网络数据传输完整性保护	
	网络数据传输保密性保护	
	网络可信接入	
安全管理中心	系统管理	安全管理平台
	安全管理	
	审计管理	
注：其中带“*”的项表示其设备的功能可在信息系统安全设计技术方案中统一考虑。		

6.3.4 第四级系统安全保护环境主要产品类型及功能

第四级系统安全保护环境中，应按照第四级系统安全保护环境的设计目标和设计策略，落实第四级安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计技术要求，选择符合相应要求的安全产品进行集成。此外，系统安全集成还应包括配置系统备份与恢复机制，支持系统管理员在系统出现故障时进行恢复；根据应用对业务连续性的要求，配置系统级的本地和异地灾难备份与恢复机制，制定应急处置和灾难恢复预案，支持应急处理和恢复。表 6-4 是第四级系统安全保护环境集成中各部分的安全功能及可供参考的主要产品类型。

表 6-4 第四级系统安全保护环境主要产品类型及功能

使用范围	安全功能	产品类型
安全计算环境	用户身份鉴别	操作系统、数据库管理系统、安全审计系统*、终端安全管理*、身份鉴别系统等
	自主访问控制	
	标记与强制访问控制	
	系统安全审计	
	用户数据完整性保护	
	用户数据保密性保护	
	客体安全重用	
	系统可执行程序保护	操作系统等
安全区域边界	区域边界访问控制	安全隔离与信息交换系统、安全网关等
	区域边界协议过滤	
	区域边界安全审计	
	区域边界完整性保护	
安全通信网络	网络安全审计	VPN、加密机*、路由器等
	网络数据传输完整性保护	
	网络数据传输保密性保护	
	网络可信接入	
安全管理中心	系统管理	安全管理平台
	安全管理	
	审计管理	
注：其中带“*”的项表示其设备的功能可在信息系统安全设计技术方案中统一考虑。		

6.4 等级保护三级应用支撑平台的设计实例

在本节中，针对一个办公自动化系统给出了三级应用支撑平台的设计实例。三级系统的关键技术是强制访问控制机制，因此，三级应用支撑平台的核心内容也是如何实施强制访问控制机制。

6.4.1 三级应用支撑平台的体系架构设计

在体系结构方面，三级安全应用支撑平台的防护体系继承了 “一个中心”保障下的“三重防护体系”架构，使得它们互为依存、相对独立。在此基础上，进一步强调了管理中心、计算环境、区域边界及网络传输的可信性，使得其在整个生命周期中都建立有完整的信任链，确保它们始终都在安全管理中心的统一管控下有序地运行，不会进入任何非预期的状态空间，从而确保了四级安全应用支撑平台的安全性不会遭受破坏，如图 6-5 所示。

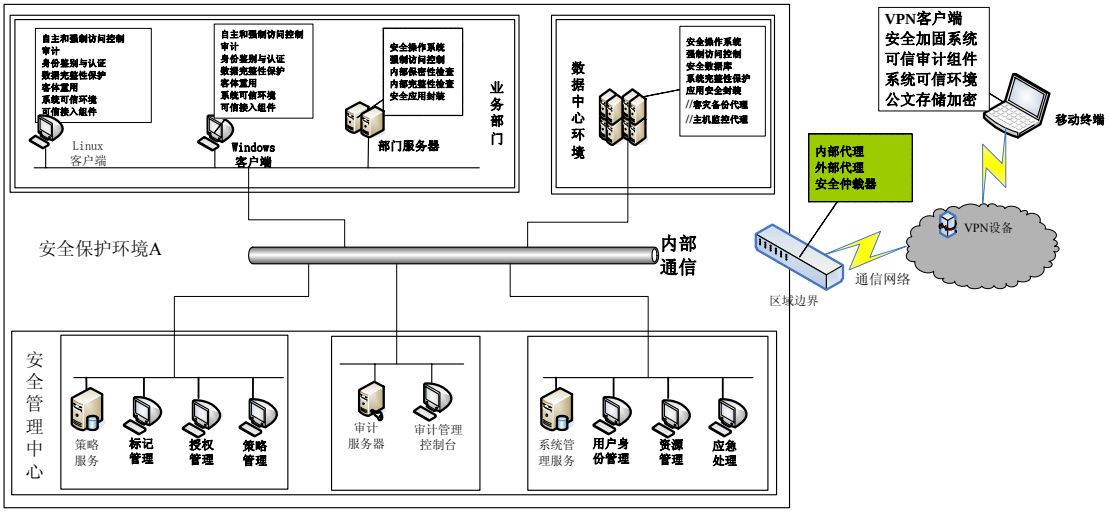


图 6-5　三级安全应用支撑平台体系示意图

本系统以第四章中提到的二维标识模型为系统的强制访问控制模型。系统中高密级的信息将标记为高保密级别，低密级的信息则标记为低保密级别。可信度较高的程序、数据标记为高完整级别，来源不可靠的数据、程序标为低完整级别。除非有安全管理中心的授权，高保密级别到低保密级别的信息流和低完整级别到高完整级别的信息流都将被禁止。

6.4.2　三级安全应用支撑平台访问控制流程

如图 6-6 所示，系统在初始化过程中，安全管理中心需要对系统中的所有主体和客体实施身份管理、标记管理、授权管理和策略管理。身份管理是确定系统中的所有合法用户的身份、工作密钥、证书等与安全相关的内容。标记管理是根据业务系统的需要，结合客体资源的重要程度，确定系统中所有客体资源的安全级，生成全局客体标记列表，同时根据用户在业务系统中的权限和角色确定主体的安全标记，生成全局主体标记列表。授权管理是根据系统需求和安全状况，授予用户访问客体资源能力的权限，生成强制访问控制列表和特权列表。策略管理则是根据节点系统的需求，生成和执行主体相关的策略，包括强制访问控制策略、级别改变检查策略等，供节点系统执行。除此之外，系统审计员需要通过安全管理中心制定系统审计策略，实施系统的审计管理。

系统初始化完成后，用户便可以请求访问系统资源，该请求将被强制访问控制模块截获。强制访问控制模块从用户请求中取出访问控制相关的主体、客体、操作三要素信息，然后查询全局主/客体列表，得到主/客体的标记信息。进而依据强制访问控制策略对该请求实施策略符合性检查。如果该请求符合系统强制访问控制策略，则系统将允许该主体执行资源访问。否则，系统将进行级别改变审核，即依据级别改变检查策略，判断发出该请求的主体是否有特权访问该客体。如果上述检查通过，系统同样允许该主体执行资源访问，否则，该请求将被系统拒绝执行。

系统强制访问控制机制在执行安全策略过程中，需要根据系统审计员制定的审计策略，对用户的请求及安全决策结果进行审计，并且将生成的审计信息发送到审计服务器存储，供审计员管理。

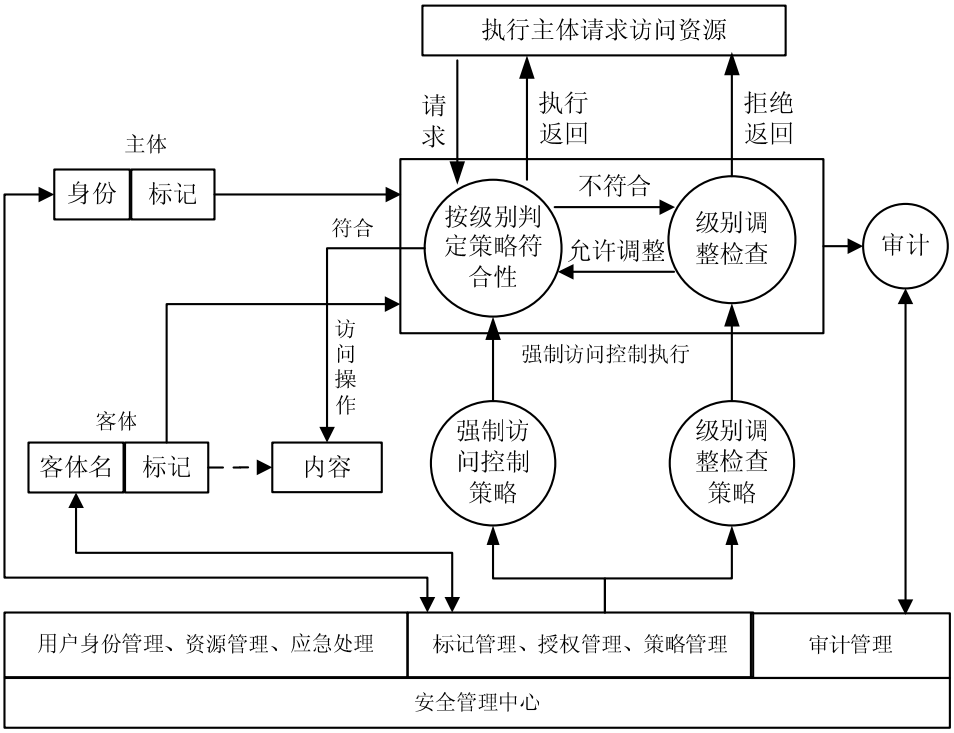


图 6-6　强制访问控制流程

6.4.3　系统组成

根据“一个中心”管理下的“三重保障体系”框架，构建安全应用支撑平台，形成安全保护环境系统，该系统分为如下四个部分：计算环境、边界区域、通信网络和安全管理中心。其中计算环境又可细分为：WINDOWS 节点子系统、LINUX 节点子系统和典型应用子系统；而作为整个三级安全应用支撑平台的核心，安全管理中心又可细分为安全管理子系统、审计子系统和系统管理子系统。

各子系统的主要功能如下：

（1）WINDOWS 节点子系统

对现有 Windows 操作系统进行安全增强，增加标记、强制访问控制、客体重用、等安全功能，增强身份鉴别机制的安全性，使其满足 GB 17859-1999 的三级要求，为信息系统的安全提供有效支撑。

（2）LINUX 节点子系统

对 Linux 操作系统进行结构化改造和安全增强，增加标记、强制访问控制、客体重用、等安全功能，增强身份鉴别级别机制的安全性，使其满足 GB 17859-1999 的三级要求，为上层应用系统的安全提供足够支撑。

（3）区域边界子系统

对流入或流出安全保护环境的信息进行安全检查，增强其强制访问控制功能，确保安全保护环境的安全性不会受到破坏。

（4）通信网络子系统

对安全保护环境间的信息流进行封装，确保信息在传输过程中不会被非授权窃听和篡改。

（5）安全管理子系统

对安全保护环境中的计算节点、区域边界、通信网络、系统管理的安全机制实施集中管理，包括标记管理、授权管理、策略管理等，为四级信息系统的安全提供基础保障。

（6）审计子系统

对安全保护环境中的计算节点、区域边界、通信网络、安全管理、系统管理统一实施与安全相关的审计管理，包括制定审计策略、分析审计结果并作报警处理，为判断系统安全状态及应急处理提供依据。

（7）系统管理子系统

对安全保护环境中的计算节点、区域边界、通信网络实施集中管理和维护，包括用户身份管理、资源管理、应急处理等，为三级信息系统的安全提供基础保障。

（8）典型应用子系统

安全保护环境为应用系统（如办公应用等）提供安全支撑服务。通过实施三级安全要求的网站应用，使用安全保护环境所提供的安全机制，为应用提供符合三级要求的安全功能支持和安全保证。

以上各子系统之间的逻辑关系如图 6-7 所示：

节点子系统通过在操作系统核心层、系统层设置以强制访问控制为主体的系统安全机制，形成了一个严密牢固的防护层，通过对用户行为的控制，可以有效防止非授权用户破坏系统的保密性和完整性安全，从而为典型应用子系统的正常运行和免遭恶意破坏提供支撑和保障。

区域边界子系统通过对进入和流出安全保护环境的信息流进行安全检查，确保不会有违背系统安全策略的信息流经过边界，是三级信息系统的第二道安全屏障。

通信网络子系统通过对通信数据包的保密性和完整性进行保护，确保其在传输过程中不会被非授权窃听和篡改，使得数据在传输过程中的安全得到了保障，是三级信息系统的外层安全屏障。

安全管理子系统是三级系统的控制中枢，主要实施标记管理管理、授权管理及策略管理等。安全管理子系统通过制定相应的系统安全策略，并且强制节点子系统、区域边界子系统、通信网络子系统执行，从而实现了对整个信息系统的集中管理，为重要信息的安全提供了有力保障。

审计子系统是系统的监督中枢，系统审计员通过制定审计策略，强制节点子系统、区域边界子系统、通信网络子系统、安全管理子系统、系统管理子系统执行，从而实现对整个信息系统的行为审计，确保用户无法抵赖违背系统安全策略的行为，同时为应急处理提供依据。

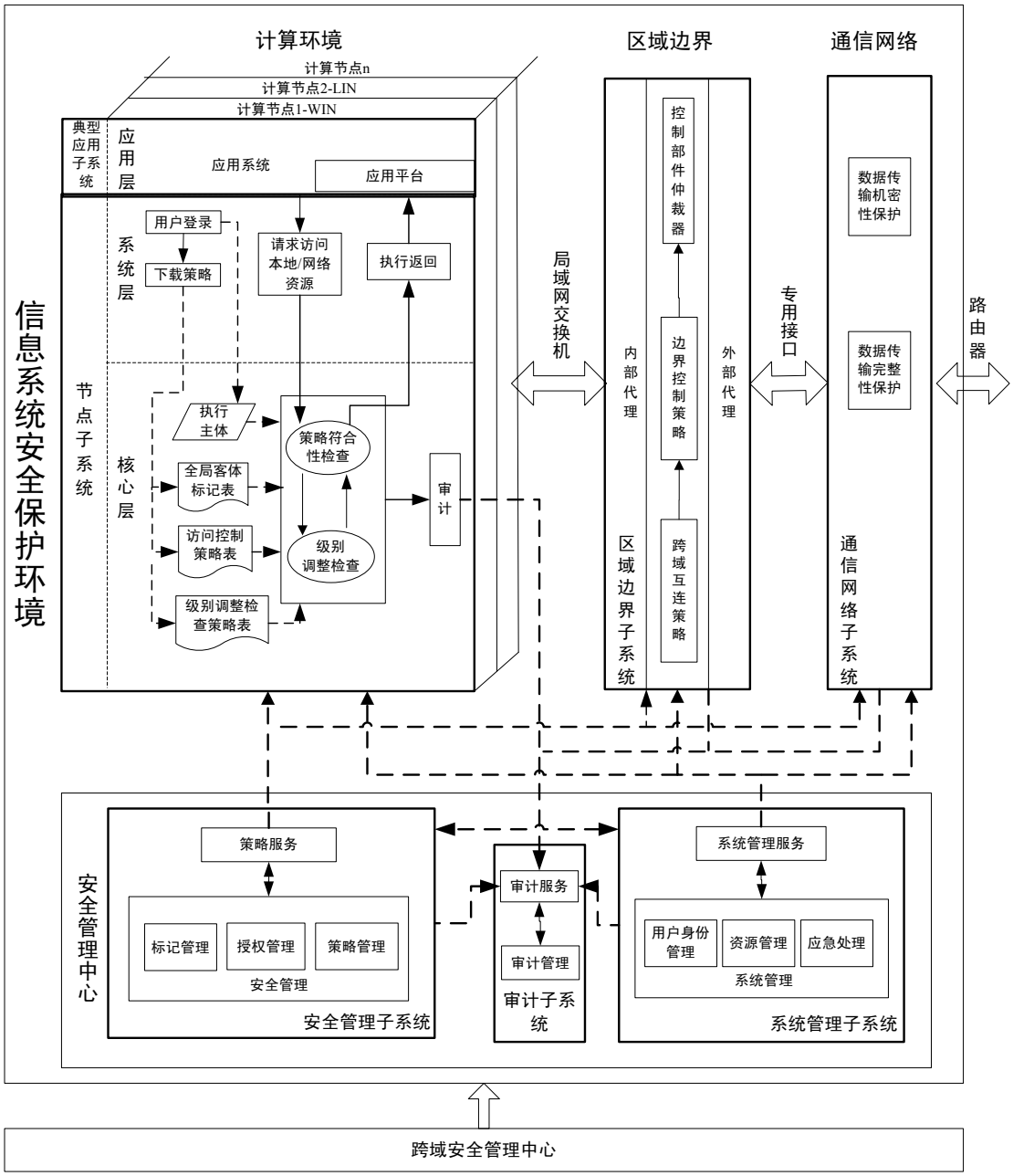


图 6-7　总体结构流程

6.4.4　总体结构流程

三级安全应用支撑平台的总体流程可以分为安全管理流程与访问控制流程。安全管理流程主要由安全管理中心的安全管理员、系统管理员和系统审计员实施，分别实施系统维护、安全策略部署和审计策略部署等机制。访问控制流程则在系统运行时执行，实施自主访问控制、强制访问控制等。

1．策略初始化流程

节点子系统在运行之前，应首先由安全管理员、系统管理员和系统审计员通过安全管理中心为其部署相应的安全策略。其中，系统管理员首先需要为信息系统中的所有用户实施身份管理，即确定所有用户的身份、工作密钥、证书等，同时需要为信息系统实施资源管理，即确定业务系统正常运行需要使用的执行程序等。安全管理员需要通过安全管理中心为信息系统中所有主\客体实施标记管理，即根据业务系统的需要，结合客体资源的重要程度，确定其安全级，生成全局客体标记列表，同时根据用户在业务系统中的权限和角色确定其安全标记，生成全局主体标记列表。在此基础上，安全管理员需要根据系统需求和安全状况，为主体实施授权管理，即授予用户访问客体资源能力的权限，生成访问控制列表和级别调整检查列表。除此之外，系统审计员需要通过安全管理中心中的审计子系统制定

系统审计策略，实施系统的审核管理。

2．计算节点启动流程

策略初始化完成后，授权用户才可以启动并使用计算节点访问信息系统中的客体资源。为了确保计算节点的系统完整性，节点系统在启动时需要对所装载的可执行代码进行可信验证，确保其在可执行代码预期值列表中，并且程序完整性没有遭到破坏。计算节点启动后，用户便可以安全地登录系统。在此过程中，系统首先装载代表用户身份唯一标识的硬件令牌，然后获取其中的用户信息，进而验证登录用户是否是该节点上的授权用户。如果检查通过，系统将请求策略服务器下载与该用户相关的系统安全策略。下载成功后，系统可信计算基将确定执行主体的数据结构，并初始化用户工作空间。此后，该用户便可以通过启动应用访问信息系统中的客体资源。

3．计算节点访问控制流程

用户启动应用后，应用代表用户发出访问本地或网络资源的请求，该请求将被操作系统访问控制模块截获。访问控制模块首先依据自主访问控制策略对其执行策略符合性检查，如果检查通过，那么该请求允许将被执行。否则访问控制模块将依据强制访问控制策略对该请求执行策略符合性检查。如果检查通过，那么该请求将允许被执行。否则，系统将对其进行级别调整检查，即依照级别调整检查策略，判断发出该请求的主体是否有特权访问该客体，如果上述检查通过，该请求同样允许被执行，否则，该请求将被拒绝执行。系统访问控制机制在安全决策过程中，需要根据系统审计员制定的审计策略，对用户的请求及决策结果进行审计，并且将生成的审计信息发送到审计服务器存储，供审计员检查和处理。

4．接入控制流程

如果主体和其所请求访问的客体资源不在同一个计算节点上，该请求将会被可信接入模块截获，用来判断该请求是否会破坏系统安全。在进行接入检查前，模块首先通知系统安全代理获取对方节点的平台身份，并检验其安全性。如果检验结果是不安全的，则系统将拒绝该请求发生。否则，系统将依据强制访问控制策略，判断该主体是否允许访问对方节点的相应端口，如果检查通过，该请求将被放行，否则被拒绝。

5．边界访问控制流程

如果主体和其所请求访问的客体资源不在同一个安全保护环境内，那么该请求必然会被区域边界控制设备截获并且进行安全性检查。检查过程类似于节点访问控制流程，不同的是，区域边界控制设备不仅接受本安全保护环境中安全管理中心的统一管理，而且需要接受上一级安全管理中心的管理，需要执行跨域互联策略，因此，区域边界从上一级安全管理中心下载策略，从跨域的角度检查是否允许该主体访问该客体资源。当检查通过后，该请求包将通过安全的通信网络传递到指定安全域中。

6.4.5　子系统接口

为了清楚描述各子系统之间的关系，这里将上述结构简化为图 6-8 所示的框图。方框表示各子系统，箭头表示各子系统之间的接口关系。

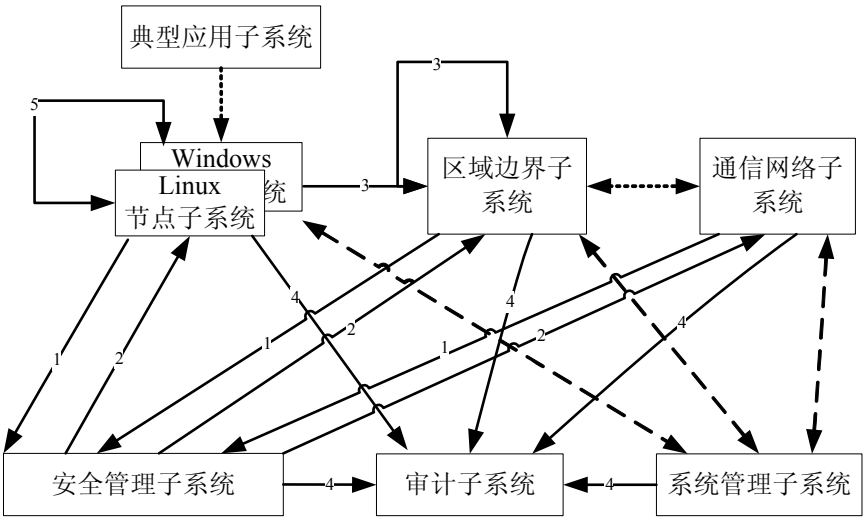


图 6-8　四级安全应用支撑平台子系统接口

典型应用子系统与节点子系统之间通过系统调用接口，其它子系统之间则通过可靠的网络传输协议（如 TCP 协议），按照规定的接口协议传输策略数据、审计数据以及一些平台认证数据，由于节点子系统与安全管理中心以及节点子系统之间的需要交换各种类型的数据，这就需要规范数据包并定义清晰的接口协议，子系统之间遵照定义的数据包结构进行数据的传输，实现审计数据的上传、策略请求和下发。限于篇幅，这里不再介绍详细的协议数据格式。

6.4.6　计算环境的设计

三级应用支撑平台的设计中，把计算环境分为 Windows 节点子系统和 Linux 节点子系统，本小节以 Windows 为例说明设计思路。

1．功能概述

GB 17859-1999 规范了三级计算机信息系统应具备的安全功能和保证功能，而安全操作系统作为信息系统安全的核心，是安全应用平台的关键支撑部件，因此其所具有的安全功能和保证功能直接影响着应用系统的安全性，直接决定了信息系统的安全强度。显然，作为三级 Windows 操作系统，它也必须满足 GB 17859-1999 规定的安全功能要求和保证要求，具体的功能要求如下：

- 强制访问控制：三级 Windows 操作系统需支持二维标识模型的强制访问控制机制，能够保护信息系统的保密性及完整性不受破坏。
- 标记：三级 Windows 操作系统需对系统中的进程、文件进行全程的标记，确保主客体在整个生命周期中其标记信息都是准确完整一致的。
- 身份鉴别：三级 Windows 操作系统应有基于可信硬件设备的安全身份鉴别机制，且可以通过安全的机制将身份与授权权限绑定。
- 审计：三级 Windows 操作系统应能对系统中所有违反安全策略的操作进行审计，并能阻止非审计管理员用户对审计信息的访问或破坏。
- 数据完整性：三级 Windows 操作系统可通过自主和强制完整性策略，阻止非授权用户修改或破坏敏感信息。

三级 Windows 操作系统主要是针对安全目的而开发，因此其指标也主要是针对安全功能和安全保证而设置，其执行性能方面则暂时不作过多考虑。三级 Windows 操作系统各功能的具体指标如表 6-5 所示。

表 6-5　三级 windows 操作系统功能指标

指标类型	指标具体内容
标记	提供二维标记，标记实体保密性级别、完整性级别、范畴。标记的对象包括系统中的用户、业务文件及进程。能够确保实体在整个生命周期中，其标记信息是准确完整一致的。
强制访问控制	强制访问控制机制实施与系统二维安全模型一致的安全策略，能够控制进程对文件的所有操作。强制访问控制机制应具有一定的灵活性，能够结合应用的流程，对进程不符合系统强制访问控制策略的行为进行检查，确保那些符合业务需求，但又不破坏系统安全的行为发生。强制访问控制机制始终有效，不会被旁路。
身份鉴别	能够提供基于可信硬件设备的安全身份鉴别机制，确保非授权用户无法访问信息系统。
审计	能够记录下述事件：用户登录事件、客体的创建和删除事件、安全管理员、安全审计员、系统操作员以及系统中其他用户的一切与安全相关的行为。审计的具体内容以满足 GB 17859-1999 中三级系统的审计规范要求。

2．组成结构

为了实现前面所述的安全功能，不仅需要对现有的 Windows 操作系统平台进行安全增强，而且需要针对特殊的应用服务程序，对其进行安全封装，以使其满足高等级的安全需求。如图 6-8 是三级 Windows 操作系统中各安全模块之间的关系图。由图可以看出，Windows 节点子系统通过在系统层增加资源访问控制功能模块以及相关的安全保障支持模块实现三级 Windows 节点所要求的安全功能和保障功能，主要功能模块包括访问控制执行模块、访问控制决策模块、安全代理模块、存储介质加密保护、身份鉴别、审计、可信接入以及可信支撑模块等。

安全代理子模块是一个系统服务程序，负责和安全管理中心、策略服务器以及其它终端平台之间的信息交互，包括标记信息的同步、安全策略的同步、可信证明的信息交互等。系统在启动过程中，安全代理模块负责从安全管理中心请求安全策略，访问控制决策模块装载由安全代理模块请求的安全

策略，并为访问控制执行模块提供安全保障服务。

三级 Windows 节点子系统在应用层通过应用服务封装实现对现有的应用服务进行安全封装，通过管道封装的形式将应用语义传递到操作系统层，从而能够更灵活地进行诸如访问控制等系统安全决策，确保在不破坏系统安全性的前提下能够更好地支撑上层安全应用。访问控制执行模块获得主体对客体资源的访问请求，并将资源访问请求发送至访问控制决策模块对访问请求进行裁决，并将结果提交审计模块进行审计。

隔离保护模块、可信支撑模块和密码支撑模块是三级 Windows 节点子系统的安全基础保障模块，保障系统的完整性和保密性。

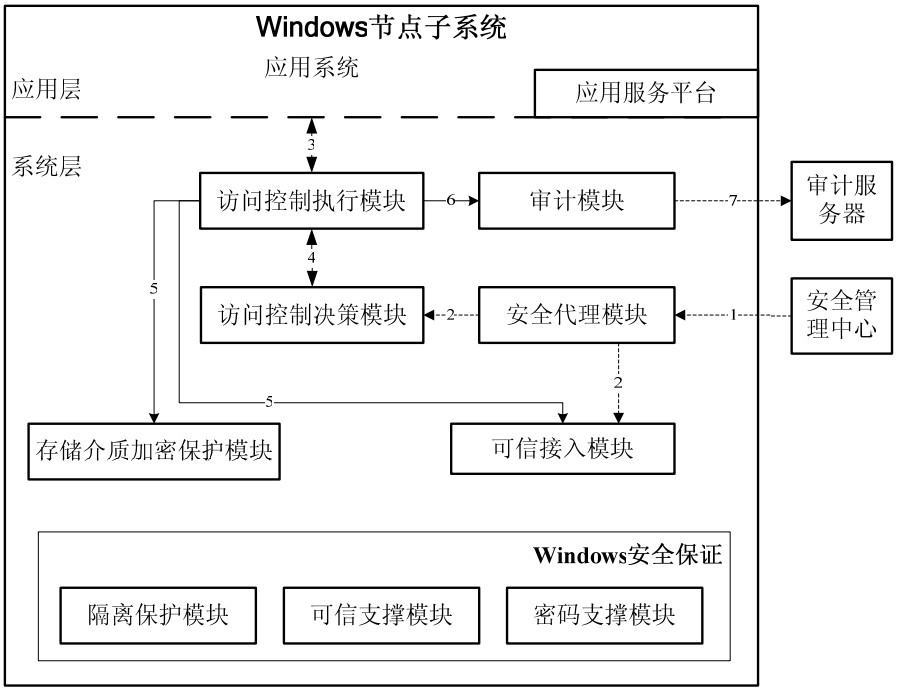


图 6-9　三级 Windows 节点子系统结构图

图 6-9 是 Windows 节点子系统模块组成图，模块是系统功能的实现，对外提供功能接口，Windows 节点子系统各模块功能描述如下：

- 访问控制执行模块：在操作系统层捕获资源访问信息，并将访问信息提交到访问控制决策模块进行裁决，根据裁决的结果决定主体对客体的访问。实现对系统重要信息的访问控制，确保信息系统的保密性和完整性不受破坏。
- 访问控制决策模块：为访问控制执行模块提供的资源访问信息提供决策支持，访问控制决策模块实现对主客体标记信息和安全策略信息的检索，并根据资源访问的主客体信息以及安全策略信息决策资源的访问，访问控制决策策略包括自主访问控制策略、强制访问控制策略以及等级改变策略。
- 身份鉴别子模块：身份鉴别子模块利用可信硬件设备，验证用户身份和用户权限的一致性，并为系统强制访问控制提供主体标识和主体权限信息。
- 审计子模块：审计子模块实现对系统中所有违反安全策略的操作的审计，向审计服务器提交审计信息，根据等级改变策略将等级修改请求提交到安全管理中心，并阻止非审计管理员用户对审计信息的访问或破坏。
- 安全代理子模块：四级 Windows 安全子系统需要与安全管理中心通信，主要包括标识同步、安全策略下载以及审计信息提交，所有这些功能的实现都依赖于安全代理子模块，安全代理子模块的主要功能是与安全管理中心、策略服务器和审计服务器的信息交换。
- 密码支撑子模块：为保证信息系统的保密性而设计的 Windows 节点子系统的密码支撑子模块是信息系统的基础保障模块。对系统信息提供透明加解密，并保证信息系统终端间的保密通

信。

- 隔离保护模块：确保系统内核、应用进程之间有良好的隔离性，屏蔽期间的恶意干扰行为。

3．工作流程

根据系统功能需求以及 Windows 节点子系统的组成结构，Windows 节点子系统的工作流程可以细化为以下三个主要的工作流程：系统登录流程、访问控制流程、可信接入流程。

系统登录流程通过用户身份鉴别模块和安全代理模块，主要完成用户身份鉴别和用户相关安全策略的下载，访问控制决策模块处理下载的安全策略。

访问控制流程是三级 Windows 节点子系统安全保障的核心工作流程，访问控制执行模块和访问控制决策模块协调一致，以实现对客体资源访问请求的控制。

下面就 Windows 节点子系统的主要工作流程做进一步描述。

1）系统登录流程

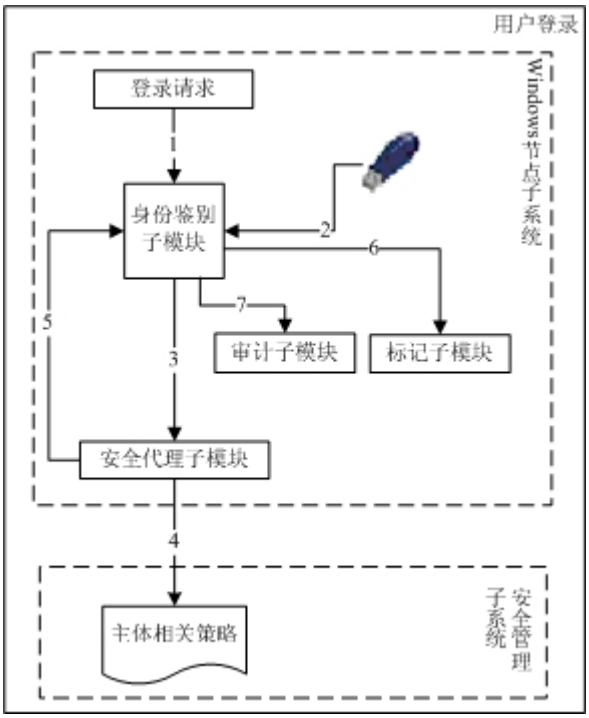


图 6-10　用户登录模块流程图

Windows 节点子系统用户登录流程如图 6-10 所示，具体流程说明：

（1）用户发出登录系统请求，激活身份鉴别子模块的用户身份认证流程。

（2）身份鉴别子模块从 USBKey 读取用户身份相关信息，该信息用于后续的认证过程。

（3）用户身份认证成功后身份鉴别子模块向安全代理子模块发送下载安全策略请求。

（4）安全代理子模块收到身份鉴别子模块的请求后，向安全管理子系统请求同步安全策略，安全管理中心将主体相关安全策略返回给节点子系统安全代理子模块。

（5）安全代理子模块将同步安全策略操作的结果返回给身份鉴别子模块。

（6）身份鉴别子模块将主体信息和客体标记提交给标记子模块。

（7）身份鉴别字模将用户登录操作提交给审计子模块，审计子模块对登录进行审计，并在适当的时候将审计信息提交到审计服务器。

2）访问控制流程

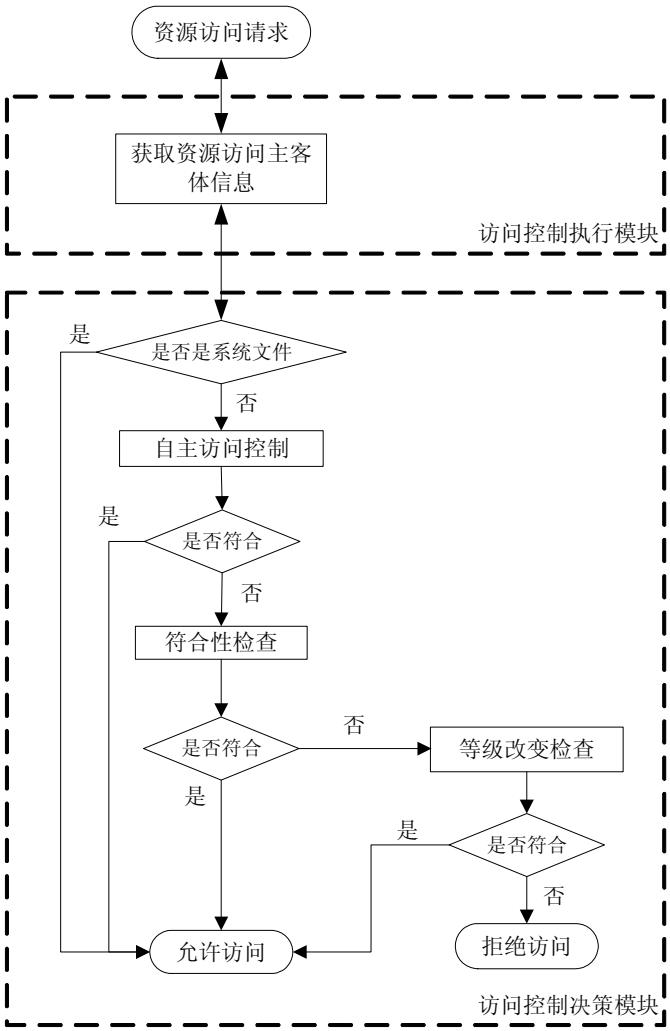


图 6-11　访问控制模块流程图

访问控制是三级 Windows 节点子系统的核心，也是三级计算机信息系统的重要内容。如图 6-11 所示，访问控制分为访问控制执行模块和访问控制决策模块，访问控制执行模块负责捕获主体对客体资源的访问信息，并将客体资源的访问信息提交到访问控制决策模块，访问控制决策模块包含主客体标记信息和访问控制安全策略的获取，并根据安全策略实现对资源访问请求的决策，在四级 Windows 节点子系统中访问控制决策策略包括自主访问控制策略、强制访问控制策略和等级改变策略。模块间关系流程如下：

（1）主体发出资源访问请求，访问控制执行模块捕获资源访问主客体信息，并将主客体信息发送到访问控制决策模块，根据访问控制决策模块裁决的结果决定是否允许对客体资源的访问。

（2）访问控制执行模块接收到访问控制执行模块的资源访问请求信息后，首先检测客体是否为系统资源，如果是系统资源则允许直接访问，否则将资源访问请求发送到自主访问控制功能模块。

（3）接着访问控制策略模块执行自主访问控制策略，符合自主访问控制策略则将请求发送到核心层，允许资源的访问，否则将资源访问请求发送到强制访问控制模块。

（4）强制访问控制模块接收到资源访问请求后，调用标记子模块，获得主体和客体的安全标记，接着进行符合性验证，在符合行验证时执行强制访问控制策略，对于符合强制访问控制策略的请求直接发送到核心层允许其对资源的访问，否则将请求发送到等级改变模块。

（5）等级调整检查模块对资源访问请求执行等级调整检查策略，也就是特权策略，资源访问请求如果符合特权策略则将请求发送到核心层允许访问，否则拒绝资源访问请求。

（6）访问控制模块将资源访问操作通过审计子模块进行审计。

6.4.7 通信网络子系统

1．功能概述

通信网络子系统负责保证安全系统在通过网络进行跨域访问时的安全，这里的网络传输安全包括数据的保密性、完整性和抗抵赖性，以及数据源身份认证和防重放攻击。具体的功能需求如下：

（1）数据源身份认证：证实数据报文是所声明的发送者发出的；

（2）数据完整性：证实数据报文在传输过程中没被修改过，无论是被故意改动过还是发生了随机的传送错误；

（3）数据的保密性：隐藏明文的消息，通常靠加密来实现；

（4）防止重放攻击：当攻击者将截获到的数据报文在稍后的时间内发送时，会被检测到，并丢弃。

由于 IPSec 能够提供以下几种网络安全服务：

（1）保密性： IPSec 在传输数据包之前将其加密，以保证数据的保密性；

（2）完整性：IPSec 在目的地要验证数据包，以保证该数据包在传输过程中没有被篡改；

（3）真实性：IPSec 端要验证所有受 IPSec 保护的数据包；

（4）防重复：IPSec 防止了数据包被捕捉并重新投放到网上，即目的地会拒绝老的或重复的数据包；它通过与 AH 或 ESP 一起工作的序列号实现。

根据以上的需求，可以考虑用 IPSec 对数据包进行加密和验证，密钥也是通过强壮的 IKE 协商的，因此可确保数据包的保密性和可信性。同时，IPSec 对数据包进行封装，隐藏数据包的一些通信特征，可抵抗通信分析。为了在不同的安全域中的透明通信，将该设备作为网关部署，这样就可以在安全保护环境之间实现安全通信，同时不影响内部的信息交换。

2．组成结构

通信网络子系统是以 VPN 网关的形式部署在应用边界之外，VPN 安全网关的系统支撑平台在基于安全操作系统的基础上，做了以下工作：

（1）面向安全网关需求对操作系统做最小化裁减安装，使得安全网关系统支撑平台为一个相对安全的操作系统。

（2）将安全网关用不到的服务统统关闭，使得安全网关的功能“有限”，将一些通用网络服务可能存在的安全隐患剔除。

（3）修改了核心模块，严格地控制了 IP 包的流向与网卡的对应关系；

（4）对内核做了安全增强，使得网关的建立在一个安全可信的专用操作平台之上。然后将 IPSec 无缝加入到内核中。

系统采用硬件加密卡进行加解密运算，加快了运算速度，也增强了安全性。加密卡是以 PCI 或者专用的接口插在主板上，在处理数据包时，模块根据密码卡要求的格式将数据包重新组织，同时告诉加密卡加密算法和密钥等信息，由硬件自动实现对数据包的加解密操作，从而提高性能和安全性。

VPN 网关的主要功能模块包括策略管理、密钥交换、加密库模块、报文封装模块、加密卡驱动。子系统的组成框图如图 6-12 所示。

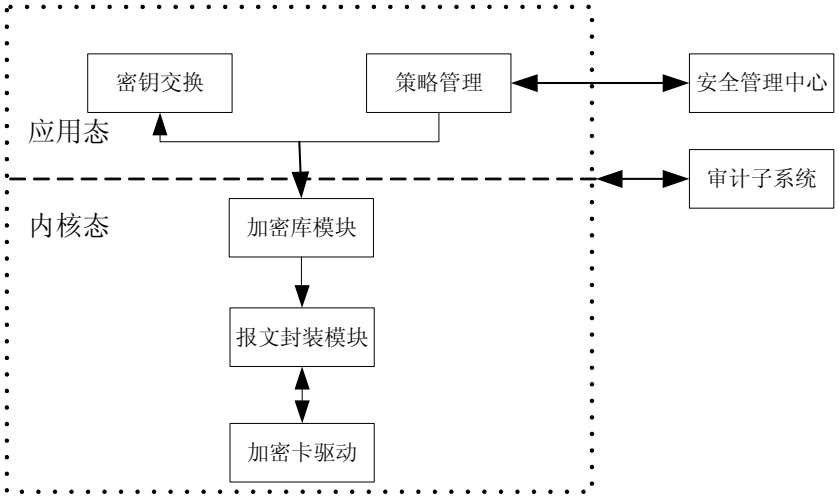


图 6-12　网络通信子系统模块组成框图

1）策略管理

从安全管理中心下载安全策略，设定 IPSec 的算法以及密钥协商和密钥的存储的位置等。

策略维护通过配置文件来实现。即用户对策略配置和管理系统进行操作实际上就是操作配置文件，但用户配置的只是配置文件中的一部分，配置文件中其它内容不允许用户改，其中包括：

（1）CA 证书、用户证书和私钥的存放位置。 CA 证书是由 CA 中心负责发放，该证书用智能卡形式发放，另外还支持由第三方提供证书来进行认证。

（2）采用 ESP 协议时，第一阶段和第二阶段的加密算法、散列算法和认证算法。

（3）连接形式：对于网关与网关之间的通信，网关总是主动连接，即 IKE 主动发起协商，试图和对方进行安全协商, 重传三次后不成功就放弃。对于网关与主机的通信, 网关是被动连接，即网关只有在接收到主机的协商消息后才和主机进行协商。

其它选项采用 IKE 里面的默认配置，如重传次数，最大交换时间等。

2）密钥交换

密钥交换模块作为一个服务运行，负责处理用户的管理配置命令，同对方设备进行密码协商交互、密钥载荷的加密验证处理以及同 IPSsec 内核的安全联盟数据库 SA 的交互。

3）密钥库模块

IPSec 内核主要包括以下几个功能：完整实现 AH/ESP 协议、维护策略库（SPD）、维护安全联盟 SA（Security Association）。在结构图中包括密钥库模块和报文封装模块。密钥库模块实现了上面的 SPD 和 SA 部分，它决定 IPSec 服务所使用的算法并放置服务所需密钥到相应位置。

IPSec 驱动模块在系统内核运行，支持传输模式和隧道模式两种安全工作模式。完成 AH 协议和 ESP 协议处理，按照 IPSec 协议标准对适当的数据包进行封装和解封操作。实现安全关联库和安全策略库，具有与 IKE 服务程序的通信借口，能够相应 IKE 服务程序的命令消息，刷新安全关联库的内容，同时也能够向 IKE 服务程序发送命令请求信息。实现验证算法和加密算法，提供算法的 API 调用接口。

可以把 IPSec 看作是位于 TCP/IP 协议栈的下层协议。该层由每台机器上的安全策略和发送、接受方协商的安全关联 SA 进行控制。安全策略由一套过滤机制和关联的安全行为组成。如果一个数据包的 IP 地址，协议和端口号满足一个过滤机制，那么这个数据包将要遵守关联的安全行为。

4）报文封装模块

该模块具体实现 IPSec 功能的 ESP 协议的处理。从 SA 中得到加密算法和密钥，对数据包进行组织，把需要加密的报文以及加密算法、加密密钥等传送到加密卡驱动，由加密卡完成加解密操作。并当加解密操作完成后，取出报文，并将报文按照既定的策略发送。

5）加密卡驱动

加密卡启动及初始化之后，加密卡驱动可管理用户提交的宏指令，驱动会将 IPSec 内核模块下发的各种命令提交加密卡执行。然后加密卡负责解释和执行用户发出的命令，且返回该命令的执行状态。

3．工作流程

初始化阶段：策略管理模块从安全管理中心和审计子系统下载相应的安全策略。

运行阶段，以输出为例，安全域 A 的主机甲生成一个 IP 包，目的地址是另一个安全域 B 中的主机乙。这个包从起始主机被发送到主机甲的网络边缘的安全网关。安全网关根据配置的策略对包进行过滤处理，看看有哪些包需要进行 IPSec 的处理。如果这个从甲到乙的包需要使用 IPSec，网关就进行 IPSec 的处理，并把报文打包，添加外层 IP 包头。这个外层包头的源地址是本地网关，而目的地址可能是主机乙的网关。现在这个包被传送到安全域 B 的网关，中途的路由器只检查外层的 IP 包头。主机乙所在网络 B 的网关会把外层 IP 包头除掉，把 IP 内层解密后发送到主机乙去。输入流程大致与输出流程一致。

对报文的具体处理过程描述：

（1）当有报文到达时，IPSec 模块根据访问控制列表（路由表）和策略库对网络接口上的数据进行选择，对禁止通行的丢弃，对允许通行的报文根据策略确定是否需要加密传输。

（2）查找 IPSec 安全关联（SA）是否已经被建立。

（3）如果安全关联已经预先由 IKE 建立，则数据包将根据安全关联中指定的算法（硬算法）对数据经行加密（转到 7），并从网络接口发送出去。

（4）如果安全关联还没有被建立，IKE 将查看是否已经建立了 IKE 安全关联。

（5）如果 IKE 安全关联已经被建立，该 IKE 安全关联将控制进行 IPSec 安全关联的协商。

（6）如果 IKE 安全关联还没有建立，IKE 将用证书认证的方式，重新协商 IKE 安全关联。

（7）将需要处理的报文按照加密卡需要的格式组织，并将加密算法和加密密钥等一同传递给加密卡驱动，由驱动给硬件加密卡进行加解密运算。

（8）当运算完成后，取出数据报文，从网络接口发送出去。

6.4.8 区域边界子系统

1．功能指标

区域边界子系统是建立在安全增强 Linux 操作系统之上的边界固化系统。系统本身的安全措施以及四级功能指标均与 Linux 节点子系统相同，在节点子系统中有具体描述。这里我们只讨论及描述对于跨边界访问的功能指标要求。

区域边界子系统根据安全管理平台所给定的访问配置策略，对所有跨边界访问的信息进行有效的安全访问控制。保障网际信息交换在安全可控的环境下进行，对访问者进行身份验证，并保留可以追究直接责任人的审计信息。保障信息交换中所保护的安全域，不受其它非授权访问的干扰和破坏。

区域边界子系统现采用三机系统体系结构：内部代理、仲裁系统、外部代理。仲裁系统和内外代理系统之间需要有安全可靠的数据传输通道，而且该数据传输通道需采用专有的数据传输协议；区域边界子系统需要获得访问主体及该主体所访问的客体信息，以对其进行访问控制。用户可以跨域访问客体，安全边界支持客体为 FTP 服务器保存的文件；WEB 服务器保存的文件（网页或者文件）；邮件服务器保存的文件（邮件）；以及协议开放的私有文件交换 CS 结构服务。

具体的功能要求如下：

（1）跨域访问控制：区域边界子系统需支持二维标识模型的强制访问控制机制，能够在跨边界访问时保护域中信息系统的保密性及完整性不受破坏。

（2）跨域访问身份鉴别：区域边界子系统应有基于安全管理策略的安全身份鉴别机制，且可以通过认证机制将身份与授权权限绑定。

（3）审计：区域边界子系统应能对经过边界的所有操作进行审计，并能阻止非审计管理员用户对审计信息的访问或破坏。

（4） 可信授权管理：只接受可信授权的系统管理，区域边界子系统应可以提供细粒度的授权机

制，使系统在制定系统安全策略时，可以逼近最小特权原则。

（5）过滤：区域边界子系统应能根据安全管理策略对信息进行一系列的安全过滤。

（6）可信接入：区域边界子系统的内部代理相对于所保护的安全域，也是其中的一子节点，因此也应符合节点与节点之间的可信互联标准。

区域边界子系统主要是针对跨边界访问的安全目的而开发，因此其指标也主要是针对跨边界访问的安全功能和安全保证而设置，其执行性能方面则暂时不作过多考虑。这里只描述了跨边界访问的各功能指标，系统本身的安全指标请参考节点子系统功能指标。

区域边界子系统跨边界访问各功能的具体指标如表 6-6 所示。

表 6-6　区域边界子系统功能指标

指标类型	指标具体内容
跨域强制访问控制	强制访问控制机制实施与系统二维安全模型一致的安全策略，能够控制进程对跨域文件访问的所有操作。并且应具有一定的灵活性，能够结合应用的流程，对跨域访问是否符合强制访问控制策略等行为进行检查，确保那些符合业务需求，但又不破坏系统安全的行为发生。跨域强制访问控制需要根据主体对跨域访问中文件、目录和设备的访问操作请求，根据安全策略对访问请求进行安全判定，对符合安全规则的请求，允许主体对资源的操作继续进行，反之则拒绝主体对资源的非授权访问。
跨域访问身份鉴别	跨域访问身份鉴别机制应能够提供基于安全管理策略配置的安全身份鉴别机制，控制允许跨边界访问的机器以及用户。在允许访问列表中的机器及用户，认证通行；不允许的则终止非授权请求。
审计	能够记录跨域访问行为中涉及到的一系列动作，包括对文件的添加删除、上传下载等操作。审计的具体内容需要满足 GB 17859-1999 中三级系统的审计规范要求。
系统可信授权管理	只可接受可信授权的管理，安全策略的制定需满足最小特权原则
信息过滤	能根据安全管理策略对信息进行一系列的安全过滤，如文件类型是否符合、关键字过滤等等。
可信接入	区域边界子系统对于保护的安全域来说也相当于其中的一个安全节点，因此需要满足节点与节点之间的可信接入。具体内容参照安全节点子系统中的说明。

2．子系统模块组成

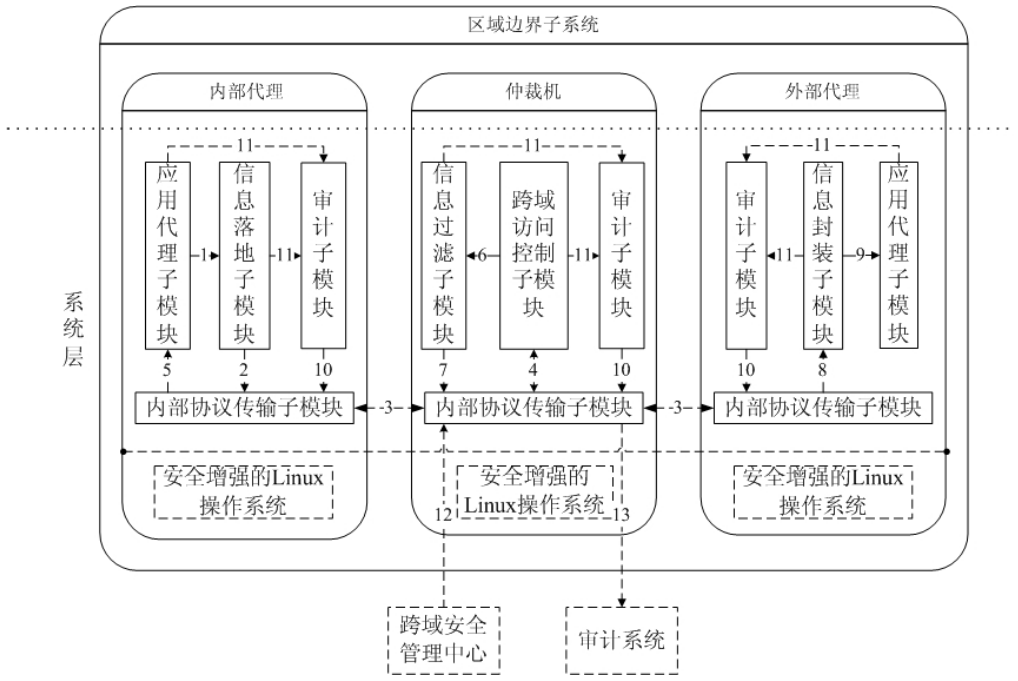


图 6-13　区域边界子系统模块组成图

图 6-13 是区域边界子系统模块组成图，其中各模块功能描述如下：

- 应用代理子模块：开启服务监听代理，接收或发送跨域网络信息。
- 信息落地子模块：还原跨域网络信息至应用层，获取主体与客体信息。
- 信息封装子模块：将允许通过的应用层数据，通过设定好的内部配置进行协议封装。
- 跨域访问控制子模块：（强制访问控制功能）根据强制访问控制策略以及主客体标记信息，实现对所保护安全域中信息的强制访问控制，确保信息系统的保密性和完整性不受破坏。（身份鉴别功能）基于安全管理策略的安全身份鉴别机制，可以通过认证机制将身份与授权权限绑定。

- 审计子模块：对经过边界的所有操作进行的审计，并向审计服务器提交审计信息。
- 信息过滤子模块：根据安全管理策略对信息进行一系列的安全过滤。
- 内部协议传输子模块：三机内部之间的数据传输。

3．子系统流程描述

1）跨域信息访问主要流程

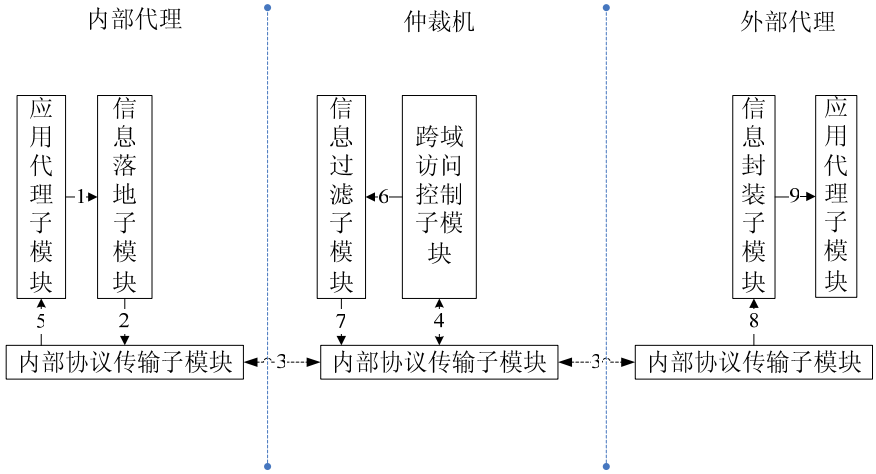


图 6-14　跨域信息访问流程图

跨域信息访问流程如图 6-14 所示，具体说明如下：

（1）首先应用代理子模块接收跨域访问信息连接，然后将信息数据交予信息落地子模块处理。

（2）信息落地子模块分析出相应的身份、主体、客体等相关信息，传送给内部协议传输子模块。

（3）内部代理的内部协议传输子模块对应用数据进行一系列的处理，摆渡至仲裁机。

（4）跨域访问控制子模块中的身份鉴别功能鉴别身份信息的合法性，判断连接的合法性，此判断结果信息用于控制应用代理子模块的通断；通过身份鉴别后，跨域访问控制子模块中的强制访问控制功能对相应的请求主体与客体信息进行访问效验，如果操作合法，则允许操作，否则中断操作。

（5）跨域访问控制的结果传回内部代理控制，采取相应的操作控制应用代理子模块。

（6）获得许可后的应用数据信息被传输至信息过滤子模块，信息过滤子模块根据过滤策略，对应用数据进行安全过滤。

（7）经过过滤的应用数据再由仲裁机内部协议传输子模块摆渡至外部代理。

（8）外部代理将应用数据按照策略配置进行数据封装。

（9）封装好的信息再由应用代理子模块发送出去。

2）安全策略获取流程

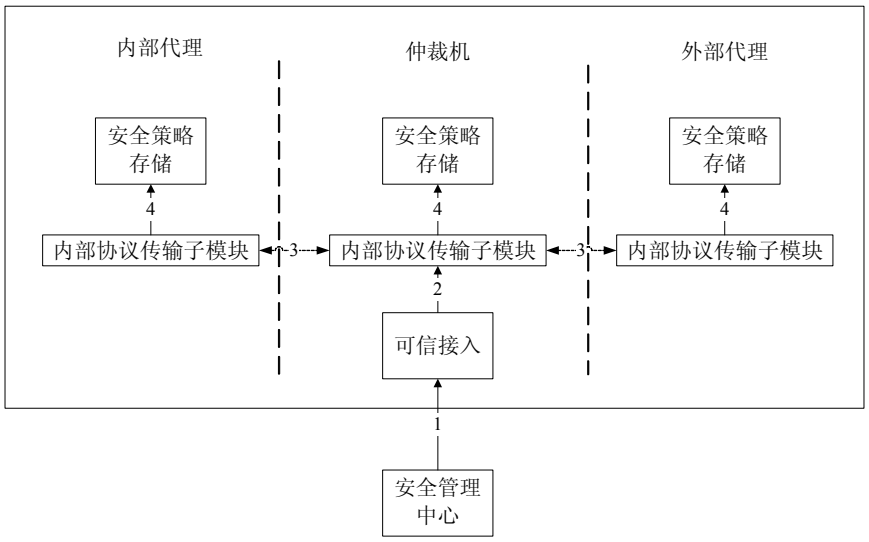


图 6-15　安全策略获取流程图

安全策略获取流程如图 6-15 所示，具体说明如下：

（1）安全管理中心与区域边界子系统接入后，先进行一系列的可信接入认证

（2）安全管理中心可信接入后，将相关的策略传送至内部协议传输子模块

（3）内部协议传输子模块将安全策略分发到内外代理

（4）各系统将所需的安全策略进行存储，以备随时被其它模块调用。

3）审计信息发送流程

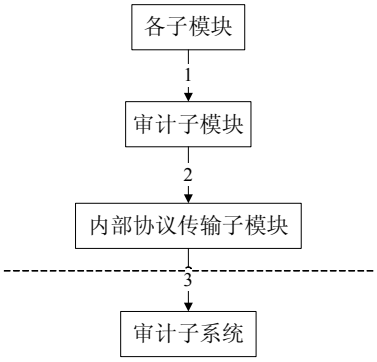


图 6-16　审计信息发送流程图

审计信息发送流程如图 6-16 所示，具体说明如下：

（1）审计子模块需要记录所有子模块所发生的一系列相关信息

（2)所有审计信息均由内部协议传输子模块传输至仲裁机。仲裁机根据相应策略进行处理及存放。

（3）仲裁系统通过统一的日志传输信道接口，将日志信息发送至审计子系统。

6.4.9　安全管理中心

1．功能概述

三级安全应用支撑平台安全管理（以下简称“安全管理”），是为三级安全应用支撑平台（以下简称“三级平台”）环境提供安全管理功能的系统，它包含主客体标识管理、授权管理，策略管理等部分，是三级安全应用支撑平台安全策略部署和控制的中心，其部署的安全策略则是连接各安全部件和各安全保障层面的纽带。

安全管理子系统策略配置包括：主体标识配置、客体标识配置、用户授权管理策略配置等；策略管理，包括安全策略的生成和下发、策略申请处理。

安全管理子系统策略配置功能如下：

- 提供用户标记管理功能，为系统中的各用户配置安全级别和安全范畴。
- 提供客体标记管理功能，为系统中与安全业务相关的客体设定安全标记，安全标记包括与文件名直接相关的安全标识、目录安全标识、通配符格式的安全标识等类型。同时提供安全标识中安全级别的修改接口，供人工参与安全级别的制定和更改。
- 提供授权管理界面，安全管理子系统提供授权模板维护强制访问控制表和自主访问控制表，将对特定客体的读、写执行等权限赋予相应的用户。对应用流程的特定位置进行授权，制定等级改变策略、网络访问控制策略等。

安全管理子系统策略管理功能如下：

- 生成访问策略库。访问策略库是将用户与用户能够访问的客体资源结合起来所形成的一个访问控制策略表，目前使用 BLP 策略模型、Biba 策略模型和二维标识策略模型，安全管理子系统根据应用的安全策略配置，生成访问策略设置，并将访问策略设置与策略配置功能所生成的用户身份配置、文件标识配置以及可信接入策略和可信进程名单等组装发送到各安全部件中。
- 策略请求和处理。策略请求和处理是将设定客体安全级别的特权和该特权所授予的用户身份结合起来所形成的一个特权列表，该列表项目来源于各用户提出的主客体安全级别修改请求

和自主访问控制策略申请，反应待定安全级别的客体资源属性和可定级主体范围，并将该列表发放到相应拥有定级权限的主体。

根据上述的安全功能要求，可以归纳出如表 6-7 所示的具体的功能指标：

表 6-7　安全管理子系统功能指标

指标类型	指标项目	指标具体内容
标识管理	主体标识管理	为用户提供直观的配置界面，配置包括用户身份对应的安全级别、用户属性等信息。 能够检查用户属性和安全级别的合规性。
	客体标识管理	提供模板编辑方式的应用文件标识管理，模板提供一组文件标识方法，其中文件名的部分字段可以以变量方式表示，由管理子系统为变量赋值，变量表示应用的具体部署方法，包括应用部署机器、目录、配置等信息。 标识管理配置界面也可以直接对文件进行标识配置，包括文件的安全级别、完整性级别和范畴。
授权管理	授权管理	以手工编辑的方式生成强制访问控制列表、自主访问控制列表、特权列表文件，（特权列表文件和应用所需特权相对应），并提供授权管理界面，由安全管理员决定特权应授予哪个用户。 执行特权授予时，应能够检查支撑应用执行的必要特权是否全部授予相关用户，并可以检查特权所授予的用户是否拥有获取该特权的权限。
策略管理	策略文件生成和下发	安全管理子系统维护一个访问策略数据库，存储用户权限、客体标识的各种信息，并可以根据访问策略设置情况，与可信网络连接和可执行代码预期值策略等组装，为每台机器生成访问策略配置文件。 安全管理子系统可以通过密码协议保护的网络通信将对应机器的访问策略配置文件发送给各机器的安全操作系统环境。
	策略请求处理	安全管理子系统接收和存储用户提出主客体标记申请和安全策略请求的各种信息，并可以转交给特权机构（用户）审核和批复。 安全管理子系统可以通过密码协议保护的网络通信将对应机器的策略请求发送给安全管理子系统，安全管理子系统通过代理发送给定级机构处理并处理返回结果。

2．组成结构

根据上述安全管理的功能，其可以分成如下一些子模块：安全管理界面子模块、授权管理子模块、标记管理子模块、策略管理子模块、审计管理子模块、策略下载请求处理模块、以及策略请求处理子模块。安全管理子系统的模块结构如图 6-17 所示：

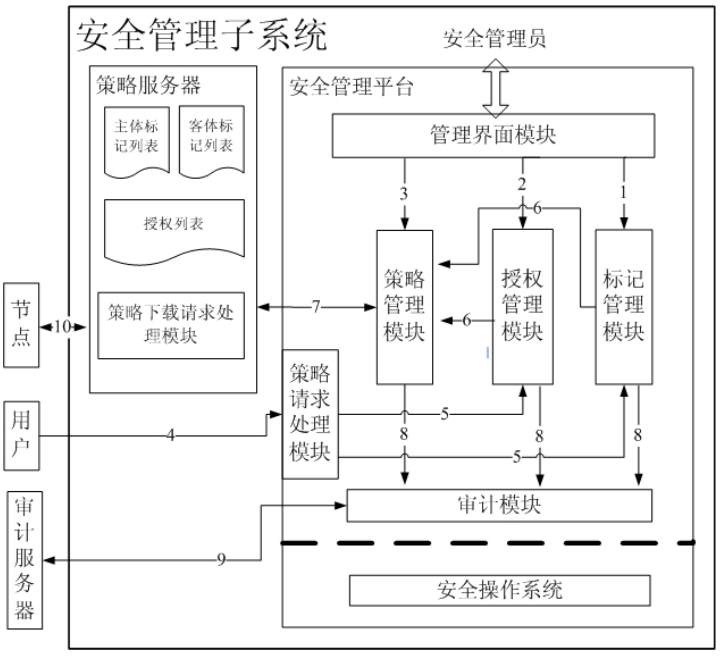


图 6-17　安全管理子系统模块结构图

安全管理子系统需连接到系统环境中。安全管理界面子模块为安全管理员提供各项安全管理功能配置接口，根据三权分立原则体现安全管理员所拥有的权限和职责。授权模块完成对用户相关权限的

管理，标识管理模块负责安全管理中心所辖的所有主客体资源的标记，策略管理子模块提供的接口函数负责安全策略的制定和维护，同时负责安全策略服务器的管理和维护。策略请求处理模块接收主客体标记和授权请求信息，然后将请求用户提出的策略请求信息转发给特权用户或特权机构，由这些特权用户对客体安全标识进行设定，返回给策略请求处理模块，然后提交给策略管理模块完成策略服务器中策略内容的更新；安全策略由策略服务器的策略下载模块发送给安全管理子系统管辖的节点、区域边界和网络设备。安全管理员的操作行为被审计模块记录并发送给审计服务器。

3．工作流程

1）标记管理流程

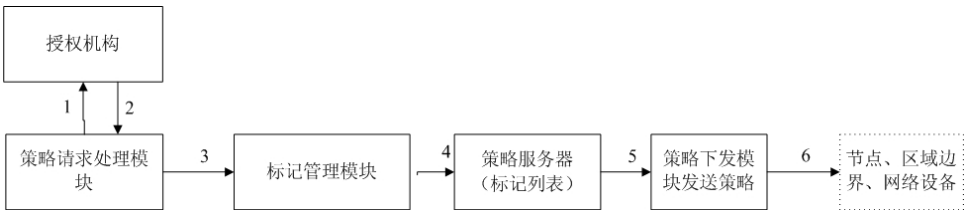


图 6-18　标记管理主要流程

标记管理流程如图 6-18 所示，具体步骤如下：

（1）策略请求处理模块接收到主客体标记请求信息，发送给授权机构（用户）审批；

（2）授权机构处理后将主客体标记信息返回给策略请求和处理模块；

（3）策略请求处理模块将标记信息发送给标记管理模块；

（4）标记管理模块对标记信息验证处理之后，经过安全管理员批准，更新策略服务器中的主客体标记列表；

（5）通知策略下发模块重新下发主客体标记列表；

（6）标记列表被发送到节点、区域边界和网络设备，更新各安全部件的标记列表。

2）授权管理流程

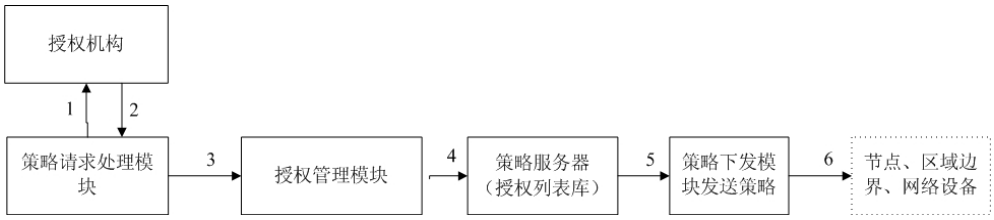


图 6-19　授权管理流程

授权管理流程如图 6-19 所示，具体流程如下：

（1）策略请求处理模块接收到对用户的授权请求信息，发送给授权机构（用户）审批；

（2）授权机构处理后将授权信息返回给策略请求和处理模块；

（3）策略请求处理模块将授权信息发送给授权管理模块；

（4）授权管理模块根据当前用户授权库对授权请求信息进行检查，保证用户授权信息符合规则；授权管理模块调用策略管理模块更新策略服务器中的用户授权列表；

（5）通知策略下发模块重新下发用户授权列表；

（6）用户授权列表被发送到节点、区域边界和网络设备，更新各安全部件的用户授权列表。

3）策略管理流程

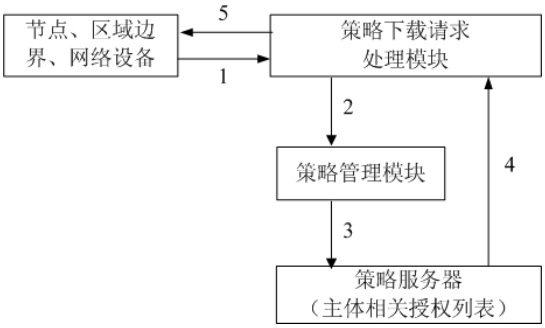


图 6-20　策略管理流程图

策略管理流程如图 6-20 所示，具体步骤如下：

（1）节点、区域边界、网络设备启动后向策略服务器的策略下载请求处理模块发送用户和节点标识信息，请求下载授权列表；

（2）策略下载请求处理模块根据下载请求调用策略管理模块对主体客体标记和授权信息列表；

（3)策略管理模块在策略服务器中的全局主客体标记列表和授权列表中选择与请求用户相关的标记列表和授权列表，并通知策略下载请求模块下发策略；

（4）策略下载请求模块从策略服务器中提取请求用户相关的标记列表和授权列表。

（5）将标记列表和授权列表下发到节点、区域边界和网络设备。

本章小结

本章介绍了信息安全等级保护，重点是高安全等级系统安全方案的设计。

本章内容主要有：

（1）信息安全等级保护综述

信息安全等级保护是国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。根据信息系统在国家安全、经济建设、社会生活中的重要程度，其遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，其安全保护等级由低到高划分为五级。

在进行等级保护技术方案设计时，要考虑以下原则：构建纵深防御体系、采取互补的安全措施、保证一致的安全强度、建立统一的支撑平台、进行集中的安全管理。

（2）等级保护安全设计技术要求

定级系统的安全保护环境是由一个中心、三层纵深防御体系构成的单一级别安全保护环境及其互联构成的。一个中心是指安全管理中心，三层纵深防御体系则由安全计算环境、安全区域边界以及安全通信网络组成。第一级系统为用户自主保护级，其核心技术为自主访问控制。第二级的关键技术为审计。强制访问控制则是三级安全系统的关键技术，也是高安全级别信息系统安全功能上的核心内容。第四级的安全功能要求与第三级基本相同，但在安全保障上有所加强，要求通过结构化的保护措施，有效加强系统 TCB 的抗攻击能力，达到防止系统内部具有一定特权的编程高手攻击的能力。第五级安全是访问验证保护级，其关键技术为访问监控器，要求基于形式化验证技术，在第四级系统安全保护环境的基础上，实现访问监控器，仲裁主体对客体的访问。

（3）定级系统安全保护环境主要产品类型及功能

不同级别的安全信息系统，需要选择相应的安全产品来实现等级保护安全机制。第一级、第二级安全系统的安全保护可以通过市场上流行的安全产品合理配置来实施，而第三级以上的高安全级别信息系统则必须基于安全操作系统，在对信息系统内部工作流程进行合理的安全分析和标识的基础上进行。需要注意，安全产品在安全保护环境中的使用并不是独立的，而必须按照保护环境的安全要求，合理配置，综合使用，最终实现对系统的整体安全解决方案。

（4）等级保护三级应用支撑平台的设计实例

本章最后针对一个办公自动化系统给出了三级应用支撑平台的设计实例。三级系统的关键技术是

强制访问控制机制，因此，三级应用支撑平台的核心内容也是如何实施强制访问控制机制。

习题

1．概述等级保护的基本概念。
2．解释为什么要实行信息安全等级保护？
3．信息安全等级保护的顶级方法是什么？
4．设计等级保护技术方案时，需要考虑哪些原则？
5．概述等级保护安全设计技术框架的主要组成。
6．等级保护各级的核心技术是什么？
7．第三级信息系统的强制访问控制功能是如何实现的？
8．举例说明如何实现第四级系统的“结构化保护”功能？
9．第四级系统中为什么不能有操作系统打补丁机制？
10．概述第二、三级系统安全保护环境集成中有哪些安全功能以及有哪些可供参考的主要产品类型？
11．概述设计三级应用支撑平台的技术要点。

第 7 章　信息系统安全工程

本章要点

- 信息系统安全工程过程（ISSE）的组成
- 系统安全工程-能力成熟度模型（SSE-CMM）的体系结构
- 系统安全工程-能力成熟度模型（SSE-CMM）的域维和能力维的组成
- 系统安全工程-能力成熟度模型（SSE-CMM）对工程能力的定级方法

7.1　信息系统安全工程基础：系统工程过程

系统工程过程是信息系统安全工程的基础，信息系统安全工程则是系统工程过程的基本原理在信息安全领域内的具体应用。本小节简介了系统工程过程的主要内容，为后续章节奠定了基础。

7.1.1　系统工程过程概况

常规的系统工程是按照如图 7-1 所示的过程而实施的。

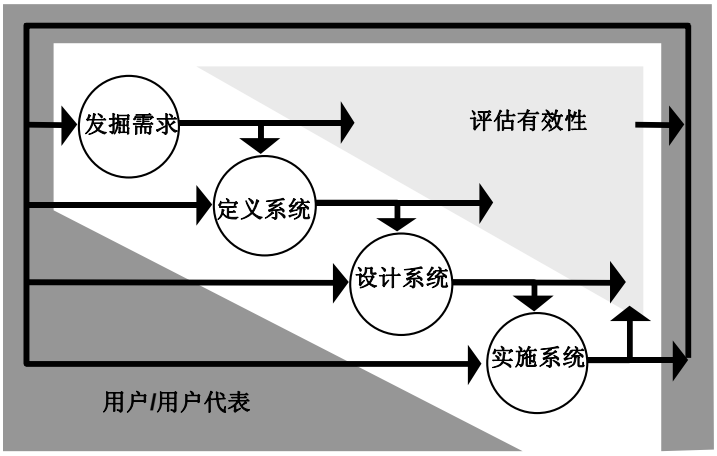


图 7-1　系统过程概况

该图所描述的系统工程过程按照下述的一般方式进行：

- 挖掘任务或业务需求
- 定义系统功能
- 设计系统
- 实施系统
- 评估有效性

这一系统工程的过程执行原则是：从“解决方案空间”中分离出“问题的空间”。问题空间表示“解决方案”这一概念的约束条件、风险、策略和一些界限。解决方案空间代表了在开发系统、满足用户需求时所有已结束的行为和创造出的产品。由解决方案空间所代表的系统工程行为和产品在开发的过程中必须不断地接受有效性评估，并判断该方案是否违背了问题空间所形成的条件。这些评估是对问题空间和解决方案空间进行必要修正的基础。从解决方案空间分离出问题空间这一原则很有意义，它便于人们制定与现有法律和政策保持一致的有效解决方案。

7.1.2　发掘需求

系统工程过程实施的起点是针对用户需求以及用户环境中的相关策略、法规和标准的一系列判断。系统工程师要标识所有的用户及这些用户与系统交互作用的基本情况，标识他们所扮演的角色、承担

的责任以及在该系统生命周期各阶段中的授权。需要发掘的需求必须来自于用户的视角，并且不应该对系统的设计与执行产生过度的约束。文档化是该过程中的一个必要步骤。文档要通过用户语言来描述工程任务或所期望的功能、现有功能的缺陷以及如何利用系统达到任务目标。

以下将介绍用于定义任务需求的主要输入以及任务描述和策略。负责执行任务的组织要能创建任务描述，更高层次的组织则应负责确定进一步的任务发展方向。最后，策略作为一种约束条件，将对系统定义、设计与实施以及系统运行、支持与处置等系统生命周期中的许多领域产生影响。

这些因素通常用于制定任务需求说明（MNS）和操作概念（CONOPS），它们将推动系统的各项特征的定义、设计与实施，使这些特征能在系统环境中成功运行。

1．描述任务/业务

在系统工程以及信息安全中，任务/业务（Commission/Business）是使用频率非常高的两个术语。这两个术语的引入反映了这样一条理念：系统过程或信息安全的全部工作都是为了使一个组织的本职任务/业务能够顺利实施。从信息化的角度讲就是：信息安全就是为信息化保驾护航，从而能使信息化最终推动组织的任务/业务。

因此，不论在本节的系统工程过程中，还是下一节的信息系统安全工程以及其它信息安全方法中，首要的一步便是确定任务/业务的需求，而不是工程或信息安全本身的需求。至于信息安全策略、目标、战略等，更是在与组织的任务/业务策略、目标、战略相一致的前提下提出的，其主旨是服务于组织的任务/业务。

一般而言，必须综合考虑各种因素来研究本组织的任务和功能。在解释为何需要某系统时，必须明确标识本组织的重要资产（例如：信息类型/包括信息处理与存储资源等网络资源在内的可用资源）。

任务描述的重点之一是对任务环境（即顺利完成任务的条件）进行描述。任务环境可以是具有竞争性的环境，例如商业行为环境；也可以是敌对环境，例如军事斗争环境。任务环境可以非常复杂——例如由常规环境变化而来的意外环境，以及变化的征兆。因此，任务描述中往往不能只描述通常所期待的常规环境、条件与规划。

任务描述也必须讨论各个利益相关者在该任务中所扮演的角色和承担的责任。例如，对于以进行装备测试为特定使命的某个敏感组织而言，任务描述必须涉及测试过程中和测试之后的信息管理方式。如果考虑一个商业组织的例子，其必不可少的一种操作就是确保资金从一个账户正确转移到另一个账户。此时，金融组织不仅应指明所有的资金转移情况，而且应指明个别资金的转移范围。一般说来，各组织必须描述其信息管理需求。需要回答的其它相关问题还包括（但不限于）：支配信息处理的规则是什么？谁具有对信息和信息资产的访问权限？这些信息和信息资产对顺利完成该任务有哪些贡献？在上述两个例子中，对相应组织尤其重要的一点是，必须描述在各种信息处理步骤中使用系统的某些个人或与系统之间存在某种交互的个人所扮演的角色和承担的责任。

2．考虑有关的政策要求

一个组织必须考虑目前所有对该组织具有约束力的政策、法规和标准。例如，国家政策、部门级别的政策、地方政策、行业政策均对一个组织具有约束力。这些都应是该组织在制定其安全策略或信息保护政策时必须考虑的因素。

在任何的系统工程过程之中，系统工程师应当认真了解这些对自己有约束力的政策，以及其它虽未明确表明（或尚未颁布）但仍有可能对系统设计造成影响的有关规定。

7.1.3　定义系统功能

1．目标

在系统开发中的功能定义阶段，系统工程师必须明确系统要完成的功能，包括该功能的实现应达到的程度以及系统的外部接口。此外，系统工程师还要将描述系统应用环境的自然语言翻译为定义接口以及系统边界的工程图表。

由需求到目的、目标到要求以及要求到功能的各进展环节均要采用工程语言。目标描述是描述对系统的运行效果的预期。系统工程师必须能将目标同此前提出的需求相联系，并且能够从理论上加以解释。各目标都有一个有效性量度（MoE）的概念，用来描述为了满足该目标而所需的条件。因此，

目标描述必须明确、可测和可验证。当所有的目标得到了满足时，如果此前从需求到目标的翻译是正确且完整的，那么这些需求能够得以满足。

2．系统背景/环境

在技术系统的背景/环境中，系统工程师要确定本系统与系统边界外元素发生相互作用时的功能与接口。系统背景/环境应当包括系统的物理边界和逻辑边界，以及系统输入/输出的一般特性。系统背景/环境还包括信息、信号、能量和资源在系统与环境或其它系统之间双向流动。系统背景/环境还应当明确，在完成用户任务时需要有哪些信息处理类型（例如对等通信、广播通信、信息存储、一般访问、受限访问等）。

3．要求

功能要求由父目标解释而来。功能要求中，需要描述系统需完成的任务、动作和行为。当其转化为性能要求时，目标有效性度量（MoE）则可用来定义功能要求的实现程度。在该阶段，除了规定系统的功能、接口、性能、互操作性以及可能的设计需求外，系统工程师也必须与用户共同决定系统开发和升级的保证要求。保证要求将影响系统设计与文件归档方法，并可使用户确信系统除了实现开发者声称的功能之外再无其它功能。这里的保证可以特指系统功能强度的性能要求，也可以特指某种用来验证并确认系统可靠性方法的处理要求。为确定一套能够满足需求的性能要求集，系统工程师在为功能要求进行性能分配时，必须进行多方面的综合考虑。一般来说，性能要求的典型形式如下：

- 质：多好？
- 量：数量，每个系统成本多高？
- 适用范围：适用范围有多大？
- 合时性：使用频度，响应度？
- 有备性（Readiness）：可靠性、可维护性、可用性、可生产性。

内部接口、外部接口与互操作性要求是系统组件之间或系统与环境、其它系统之间的互作用概念的重要要求。此外，某些政策法规也可能对一些接口、互操作和设计要求造成影响。为了实现系统功能，系统工程师需要从这些要求出发进一步提出其它要求。

当明确所有要求之后，系统工程师必须同其他系统负责人商议并评估这些要求的正确性、完整性、一致性、互依赖性、冲突和可测试性。能够正确解释目标的要求应做到既不苛刻，也不模糊。极端苛刻的要求可能会对一些系统性能提出过高的要求，并且可能会影响到其它某些合理要求的实现。各种要求必须是一致的。对用户、客户或开发者而言，它们代表了同一个具体事物。系统工程师必须解决不同要求之间的冲突，并通过与其他系统责任人进行协商的方式淘汰和修改某些要求。用户应该区分要求的优先级，在发生冲突的情况下，可以在必要时放弃低优先级的要求，以此缩短时间、降低成本、减缓风险和缩小范围。尤为重要的一点是，由于需满足的要求是系统有效性和可用性的基础，系统负责人必须在这些要求及其特性上取得一致意见。

这个阶段中应当创建要求跟踪矩阵（RTM），用以对系统功能要求的定义过程进行跟踪。而且，因为功能要求是有效性的基础，故在 RTM 中必须包括对每一要求或要求集的测试计划。

4．功能分析

功能由要求而决定，每个要求将产生一项或几项功能。初始功能的级别高低与功能和要求的描述方式有关。功能分析的主要内容是分析功能之间或功能与环境之间的联系。

有很多方法可以通过图表来描述功能的相互联系。最简单的图表是文本功能列表，它通过习惯性的缩进、标号、字体来描述一系列功能的层次结构。功能列表将对功能进行命名，并且描述其定义、行为、何时被调用以及输入输出。例如，“能量转换”功能（发电机）需要详细描述输入条件和能量（将机械能量输入的装置）以及相应的输出条件和能量（将交流电作为输出的转换装置）。

由于功能列表具有分层的特点，它也可以是一个树型结构。应将重要功能及其继承功能分组，使它们之间保持高度的独立性，这是定义模块化结构的基础工作。模块化结构具有连带关系（每一个模块或子系统产生一个系统功能，该系统功能由紧密联系的低层功能构成），同时也具有弱耦合结构（各模块或子系统之间在很大程度上保持相互独立）。系统工程师必须在连带和耦合之间进行平衡；模块化

系统几乎可以与独立的子系统一样便于定义、设计、开发、测试、移植和升级。通过这种平衡可以产生各种可能的系统结构，这样便实现了用来分配功能的子系统和底层组件的可视化。

接口描述的可视化可以通过画 N2、功能流框图和背景图表实现。N2 框图的一个坐标（通常是纵坐标）表示功能输入，另一个坐标（通常是横坐标）表示功能输出。它可显示各功能与其它功能之间的依赖关系。对于较简单的系统设计，N2 框图中远离对角线的输入输出交叉点也较少。在功能流框图中也可以描述接口，还可以描述复杂度和过程流。背景图表则是在与之相关的其它系统或环境背景下描述系统，通过建立低层背景图表便能够明确外部功能接口的特定性能。

7.1.4 设计系统

此部分工作需要一个涵盖多学科知识的工作组来设计系统的体系结构并制定具体的设计方案。系统工程师要对体系结构进行分类，并标识所有类似的可重用方案。此时，系统工程师可以组织一个负责开发具体解决方案的工作组。该工作组将负责选择可用于该方案的产品，采用裁剪可重用方案或设计新方案的方式设计具体的体系结构解决方案。

一个系统的运行必须依赖其所有组件，因此，耗费过多精力对某个组件进行优化并不可取。但是，性能过低的组件也可能会损害到系统的整体性能。系统设计必须满足包括功能、性能、接口、互操作和设计要求在内的一系列要求。

1．功能分配

在这个过程中，系统工程师必须明确各组件在实现其功能时应采取的物理形式。他们可以将一些功能分配给软件、硬件、固件和人。执行系统功能的人一般都采用确定的工作程序与书面步骤，使用特定的可用软件、硬件与固件。当功能被分配给组件后，各组件必须确保能实现相应的功能和性能要求，并且能不超出系统规定的出错率。系统工程师必须在体系结构层面说明如何将功能和要求分配给各个组件，并同系统负责人对概念和物理上的可行性取得一致意见。

此时，系统工程师可以考虑系统的验证、集成和有效性测试计划，并与要求和体系结构相联系。系统工程师还可以开始针对系统设计来分配资金、人员、工具和时间资源，用于系统的测试、后勤、生命周期支持。多数系统需要有正式的配置管理（CM），并将 CM 作用于体系结构。

2．概要设计

进行系统概要设计至少应具备两个先决条件：明确且达成一致的系统要求；配置管理下的确定的体系结构。一旦体系结构已经确定，系统和设计工程师就必须制定用于具体描述系统建设内容的规范。该规范必须同 RTM 规定的需求密切相关，且具有内在完备性和一致性。规范的粒度级别应从系统级逐渐流向组件级。此外，应当在概要设计审查阶段（PDR，Preliminary Design Review）之前对更高级规范进行制定和评审。PDR 产生的高级规范将用于调查完备性、冲突、兼容性、可验证性、安全风险、集成风险和可追踪性等要求。

3．详细设计

详细设计将产生更低层次的产品规范、具体的工程与接口控制图、原型、具体的测试计划与流程和具体的集成后勤支持计划（ILSP，Integrated Logistics Support Plan）。可靠性、可维护性、可用性、质量、安全性和可生产性均是重要的参考，可用于确定购买或开发系统的具体内容与方式。详细设计阶段还要实施系统关键设计审查（CDR，Critical Design Review）。审查内容涉及到所有配置项（CI，Configuration Item）的具体规范，涉及到完整性、冲突、兼容性（与接口系统）、可验证、安全风险、集成风险和可追踪性等要求。

7.1.5 实现系统

系统实施的目的是为所设计的系统开发并集成其全部组件。一旦该过程结束，下一步工作便是对系统进行测试和验证，确定系统是否满足要求。这个工作也包括对建设该系统的可能性进行调查。

系统实施行为将得出系统验证审查（SVR，System Verification Review）结论，它为所建立的系统是否遵循系统设计要求并满足任务性能需求提供了证据。

1．采购

本阶段的工作必须在开发或购买能够满足系统规范的组件这二者间作出决定。在选择解决方案所

需的集成产品时，要以详细的设计方案为基础。这些产品可以通过购买、租用、借用的方式获得，具体方式取决于很多已知因素（组件价格、是否容易获得、形式、是否合适、功能等等）或未知因素（在具体系统中的可靠性，组件性能的不足可能对系统性能造成的风险，该组件将来是否可用或可被替代等）。在正式决定开发或购买之前，系统和设计工程师必须慎重权衡两种方式的利弊并进行深入研究。

2．建设

在本阶段，已制定的各种系统规范将被转化为一个稳定的、可生产的、性能代价比合理的系统设计实践。对信息系统而言，这种转化涉及到了所有产品级的软件、硬件和固件。

一旦组件的采购和交付过程完成，系统工程的下一步工作就是装配或建设系统。在此之前需要验证各组件是否符合相应的系统设计规范。验证结束便可以开始建设系统。

3．测试

完成组件开发后，必须对组件开发结果进行测试。系统和设计工程师要制定测试过程和预期的测试结果，设计工程师还要进行单元测试，这确保了所有的组件能够正确实现其功能。需要注意的是，在验证和集成测试过程中还必须对所有接口进行全面测试。

集成测试是组件测试之后的更全面、深入的测试。必须事前规定系统集成测试所需的人员、工具、设备、资金资源，做好预算。集成测试可能导致要改变某些系统组件，这需要立即反馈给系统设计，以供其作出判断。该阶段要形成一份系统功能测试报告，用于记录测试结果。

一般说，任务需求还可能要求开发一些特殊系统，或者该系统将被用于某个未知或难以模拟的环境。此时，必须针对实际系统进行在线测试。当很多相同的系统部署于某个已知且可模拟的环境时，也应在每次生产和部署之前进行仔细测试。

在对系统验证之后，尤为重要的是针对系统的安装、操作、维护和支持步骤进行归档。这些步骤将以需求、体系结构、设计和针对系统建立之初的配置所进行测试的结果为基础。需要重点指出的是，在安装过程中必须记录异常情况，并且关注这些变化对系统集成以及操作所可能产生的影响。此外，还要分析安装过程中的变更情况对系统操作、支持与维护可能造成的其它风险。

7.1.6　有效性评估

在评估系统有效性时，必须检测两个主要的因素。第一，系统是否达到了任务的需求？第二，系统是否能够依照组织所期望的方式操作？系统功能和操作需求是系统建设成败的主要因素。除这些因素之外，还应该注意可能影响评估结果的如下因素：

- 互操作性。系统能正确地通过外部接口共享信息吗？
- 可用性。用户能够使用系统来提高任务的成功性吗？
- 训练。用户要合格地操作和维护系统需要何种程度的指令？
- 人机接口。人机接口问题是否会导致用户出错，从而对系统和任务不利？
- 成本。建立、更新和维护系统是否具有经济上的可行性？

7.2　经典信息系统安全工程（ISSE）过程

7.2.1　ISSE 概述

信息系统安全工程（ISSE）是美国军方在 20 世纪 90 年代初发布的信息安全工程方法，反映 ISSE 成果的文献之一是 1994 年出版的《信息系统安全工程手册 v1.0》。该过程是前述的系统工程在安全空间的映射，其重点是通过实施系统工程过程来满足信息保护的需求。ISSE 将有助于开发可满足用户信息保护需求的系统产品和过程解决方案，同时，ISSE 也非常注重标识、理解和控制信息保护风险并对其进行优化。ISSE 行为主要用于以下情况：

- 确定信息保护需求；
- 在一个可以接受的信息保护风险下满足信息保护的需求；
- 根据需求，构建一个功能上的信息保护体系结构；
- 根据物理体系结构和逻辑体系结构分配信息保护的具体功能；
- 设计信息系统，用于实现信息保护的体系结构；

- 从整个系统的成本、规划、运行的适宜性和有效性综合考虑，在信息保护风险与其它 ISSE 问题之间进行权衡；
- 对其它信息保护和系统工程学科进行综合利用；
- 将 ISSE 过程与系统工程和采购过程相结合；
- 以验证信息保护设计方案并确认信息保护的需求为目的，对系统进行测试；
- 根据用户需求对整个过程进行扩充和裁剪，为用户提供进一步支持。

为确保信息保护能被平滑地纳入整个系统，必须在最初进行系统工程设计时便考虑 ISSE。此外，要在与系统工程相应的阶段中同时考虑信息保护的目标、需求、功能、体系结构、设计、测试和实施，并基于对特定系统的技术和非技术因素的综合考虑，使信息保护过程得以优化。

ISSE 的主要原则有：

（1）始终将问题空间和解决方案空间相分离。

“问题”是“我们期望系统做什么？”“解决方案”是“系统怎样实现我们的期望？”当人们关注解决方案时，很容易忽视对问题的注意，这往往会导致错误问题的解决和错误系统的建造。如前所述，系统工程界的共识是：“没有比解决一个错误的问题并建造一个错误的系统更低效的了。”

（2）问题空间要根据客户的任务或业务需求来定义。

客户经常同工程师讨论技术或对解决方案的想法，而不是告诉工程师问题在何处，这也是系统工程领域存在的突出现象。系统工程师和信息系统安全工程师必须把客户的这些想法放到一边，发掘出客户的基本问题。如果客户的需求不是基于其任务或业务需求而提出的，则最终系统可能难以满足客户的需求。这样会继续导致错误系统的建造。

（3）解决方案空间要由问题空间相驱动，并由系统工程师和信息系统安全工程师来定义。

是系统工程师精通系统的解决方案，而不是客户。显然，如果客户是解决方案的设计专家，那就没必要再去雇用系统工程师了。一个坚持介入设计工程的客户很可能会对解决方案带来限制，影响到系统工程师的灵活性，从而影响到系统的任务或业务支持目标，最终影响到用户需求的满足。

7.2.2 发掘信息保护需求

“发掘信息保护需求”是 ISSE 过程中的第一项活动，相应的系统工程活动称为“发掘需求”（见图 7-1）。如果“发掘需求”的活动没有实施或实施不彻底，信息系统安全工程师必须完成下述系统工程任务：

- 理解客户的任务或业务。
- 帮助客户判断其任务或业务需要何种信息管理模式。
- 创建信息管理模式，获得用户认同。
- 记录上述结果，以判断信息系统是否能够满足客户需求。

为了理解客户的任务或业务，信息系统安全工程师必须充分利用所有可能的资源，例如客户的制度规定、年度报告以及某些其它文档。可以在类似于任务需求说明（MNS）或高级运行概念（CONOPS）等文档中对任务或业务作出记录，但最重要的信息来源是直接同客户沟通。

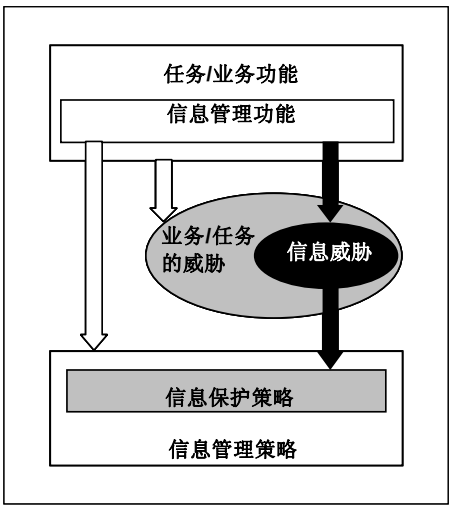
为了定义信息管理需求，应制定信息管理模型，在其中标识出处理过程、被处理的信息以及用户。该模型事实上是一种结构化的分析，用来将用户的角色、过程、信息进行分解，直至清晰且无歧义。在建模过程中，重要的一步是应用“最小权限”规则，即用户只能接触为完成其工作所必不可少的过程和信息，不能拥有过度的权限。模型中还应包括所有的信息管理策略、规则和约定以及对被管理的信息提出的要求。该模型的主要组成是信息域，每一个信息域中要确定以下 3 类要素：

- 信息域的用户或成员。
- 适用于信息管理用户的规则、权限、角色和责任。
- 被管理的信息对象，包括过程。

模型便是这些信息域的集合。产生的 IMM（信息管理模型）文档通常非常详细地描述了信息管理的需求。信息系统安全工程师可以对系统工程师开发 IMM 的过程提供支持。图 7-2 简单描绘了“发掘信息保护需求”的活动。

图 7-2　发掘需求

IMM 完成后，信息系统安全工程师就可以在此基础上明确可行的保护策略、安全规则、必须遵循



的法规等。IMM 文档中还可以定义所需的安全级。

“发掘信息保护需求”的一项关键活动是定义信息面临的威胁。这时可将客户作为最好的知识源，并通过信息系统安全工程师的专家经验进行指导，为每一个信息域指定信息受到的危害的度量准则和可能的危害事件，这项工作要结合等级保护工作进行。

ISSE 将信息威胁作为设置保护优先级的出发点，据此定义安全服务的类型及强度。信息系统安全工程师和客户将对每一个威胁应用保密性、完整性、可用性、访问控制、标识和鉴别（I&A）、不可否认性和安全管理等服务。服务的强度要与信息威胁的等级相适应。

ISSE 的所有阶段中，文档均是必不可少的关键要素。在发掘信息保护需求时，信息系统安全工程师要将信息威胁、安全服务的类型和强度及优先级、角色与责任记录下来。其中，客户的任务或业务支持系统面临的信息威胁及相应的安全机制要以信息保护策略（IPP）的形式予以记录。在取得客户的认同后，IPP 就成为了客户的信息管理策略的一部分，在其余 ISSE 活动中，这是评估信息保护有效性时的基础。图 7-2 刻画了由组织的任务或业务到 IPP 的过程流。

在工程过程的早期阶段，信息系统安全工程师还应开始对设计约束进行定义。这些约束可以来自于此前标识的法律法规要求之中，也可以继承自必须与目标系统相接口的既有系统。这些约束必须得到明确记录，并在整个 ISSE 过程中受到追踪。

信息系统安全工程师负责向用户提出工程过程、概括信息模型、确定威胁和安全服务并判断出威胁和服务的相对强度和优先级。这是对客户的信息管理和保护需求的记录，是后续所有开发活动的基础，因此客户对这些结论的认同至关重要，这也是信息系统安全工程师的工作效果的测度。

7.2.3　定义信息系统安全要求

这项活动是系统工程中“定义系统要求”的对应。信息系统安全工程师要在该阶段考虑一套或多套能够满足由客户提出并记录在 IPP 中的信息保护需求的解决方案集。图 7-3 中阐述了信息保护需求和解决方案之间的映射。每一个解决方案集都要定义下述目标系统的概念：

- 系统背景环境。
- 概要性的 CONOPS。
- 系统要求（如何实现系统）。

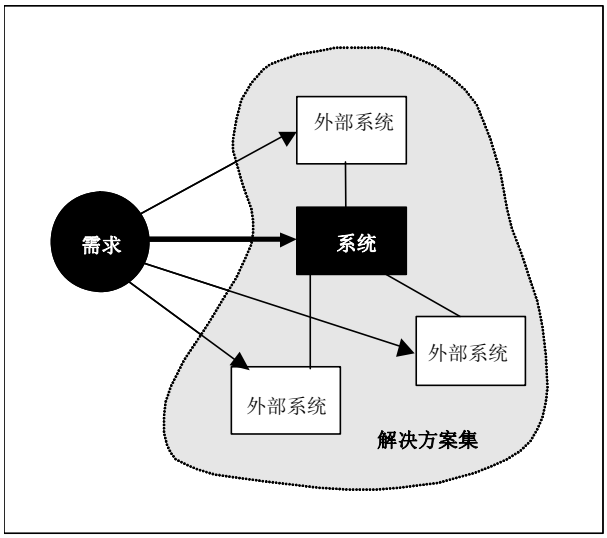


图 7-3　将需求分配解决方案集中

在客户的参与下，信息系统安全工程师需要选择一套解决方案集，记录下系统的背景环境、CONOPS 以及安全要求。这项活动完成后，可能需要对现有系统作出变动或开发多个目标系统。图 7-3 还展示，信息保护的需求不一定要分配到目标系统中，还可以分配给外部系统。例如，PKI 便是典型的外部系统。

在确定系统的安全背景环境时，需要定义系统的边界，并将安全功能分配到目标系统和外部系统中，标识出目标系统和外部系统之间的数据流以及这些数据流的保护需求。IMM 中的信息管理需求以及 IPP 中的信息保护需求均要在目标系统和外部系统中进行分配。在外部系统中的功能分配必须得到该系统所有者的同意。系统安全背景环境文档应记录这些分配情况，规定出目标系统与外部系统间的数据流及其控制方式。

CONOPS 将从用户的角度描述系统的任务运行所需的信息管理和信息保护功能，但不必定义一步步的流程。CONOPS 要说明对其它系统的任务或业务的依赖性以及由这些系统交付的产品和服务。系统安全背景环境和 CONOPS 要与系统工程师、客户以及外部系统的所有者相协调。

信息系统安全工程师应与系统工程师合作定义系统要求、系统安全运行模式以及系统的性能指标。系统要求中应该规定出系统必须完成的事情，而不是去设计和实现系统。系统工程师和信息系统安全工程师必须确保这些要求是可理解的、无歧义的、综合的、全面的和简洁的。系统要求的分析中必须定义系统的功能要求和设计约束。功能要求的目的是定义数量（多少）、质量（多好）、覆盖面（多远）、时间线（何时以及多长）以及可用性（多久可用）。此外，性能要求以及设计约束也要成为系统要求文档的一部分。设计约束不能与系统的实现相独立，它要影响到设计决策以及部分的系统设计。设计约束还包括由外部系统施加的约束，并应与系统的接口要求相独立。设计约束中需定义的内容包括：限制设计灵活性的因素，例如环境条件或环境限制；内外部的威胁场景；以及合同、惯例或法规标准等。系统要求在获得批准后要作为设计者进行系统开发的基线。

在要求的分析过程中，系统工程师要审查可追踪性文档，确保发掘出的所有需求都已经分配到了目标或外部系统之中，确保目标系统的背景环境描述中包含了所有的外部接口和信息流。系统工程师还应确保概要性的 CONOPS 能覆盖所有的功能性和任务或业务需求，并且系统运行的内在风险也得到了考虑。

信息系统安全工程师要确保所选择的解决方案集能够满足任务或业务的安全需求，系统边界已经得到协调，并确保安全风险可以达到可接受的级别。信息系统安全工程师要将安全背景环境、安全 CONOPS 以及系统安全要求提交给客户，并得到客户的认同。

7.2.4　设计系统安全体系结构

在系统工程的“定义系统要求”活动中，系统要求要分配到整个信息系统中，它只是指明了系统的功能，却没有定义系统的组件。而在“设计系统体系结构”活动中，系统工程小组将要对功能进行分解，选择具体功能的执行组件，这是体系结构设计的核心内容。图 7-4a 和 7-4b 描述了“定义系统要求”与“设计系统体系结构”的区别。前者将目标系统视为“黑盒”，后者则创建系统的内部结构。同样的对照也发生在 ISSE 的相应活动中：“定义系统安全要求”与“设计系统安全体系结构”。

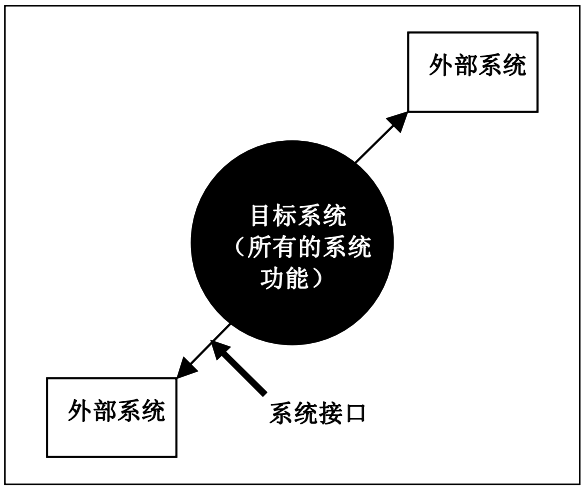


图 7-4a　定义系统要求

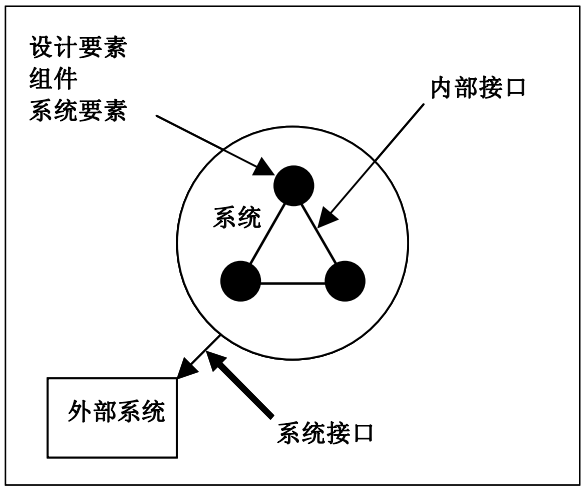


图 7-4b　设计系统体系结构

功能分析要将此前的要求分析阶段所确定的高层功能分解至低层功能，与高层功能相关的性能要求也要分解至低层。功能分析的结果是描述每个产品或项目的逻辑功能或性能。分析的对象包括待建系统的体系结构、功能和过程、接口（内部和外部）、元素（组件）、信息的流动情况、环境和用户/访问。

上述描述通常称为产品或项目的功能体系结构。功能分析和分配使得可以对系统的功能目的及其实现方式形成更好的理解，并在一定程度上获知低层功能的优先级和可能存在的冲突。它提供了对于优化物理解决方案来说重要的信息。功能分析和分配过程中使用的关键工具是“功能流块图”、“时间线分析”以及“要求分配表”。

在本项活动中，信息系统安全工程师要与系统工程师合作，确保安全要求能正确地流向体系结构，且体系结构不会对安全造成削弱。

信息系统安全工程师要负责向目标系统和外部系统分配安全要求，并确保外部系统可以支持这些安全要求。就安全而言，这尤为重要，因为密钥管理等安全服务通常要分配给外部系统。

信息系统安全工程师还要在此项活动中确定高层安全机制（例如加密和数字签名），这样，安全机制间的依赖性，例如密钥管理和加密，才能得到讨论和分配。信息系统安全工程师还要将安全机制与安全服务的强度相匹配，落实设计中的约束因素，分析并记录下发现的不足，实施互依赖分析，确定安全机制的可行性，并评估这些安全机制中存在的任何残余风险。体系结构中不涉及安全机制的具体实现，所以风险分析过程所需的详细的脆弱性和攻击信息是不能在该活动中提供的。然而，有经验的信息系统安全工程师可以在风险分析中描述出组件中可能存在的脆弱性和攻击的大致情况。

风险分析过程可以确保所选择的安全机制能够提供预期的安全服务，有助于向客户解释安全机制对安全要求的满足程度。体系结构对这些要求的有效性要以风险分析的结果以及客户是否认同本阶段中建议的行动路线为评价。

7.2.5　开展详细的安全设计

信息保护的设计是一种不断反复的过程，涉及到了系统工程与信息系统安全工程组的交互以及工程组内系统工程师和组件工程师之间的交互。要做出合理的设计决策，需要 ISSE 工程组不断地实施评估，以比较系统安全要求中的预期风险。

在“开展详细的安全设计”活动中，信息系统安全工程师要确保对安全体系结构得到了遵循，实施均衡取舍研究，并定义系统安全的设计要素，包括——

- 向系统安全设计要素中分配安全机制。
- 确定备选的安全产品。
- 确定需要定制的安全产品。
- 检验设计要素和系统接口（内部及外部）。
- 制定安全规范。

信息保护的设计阶段将规定系统及其组件，但不必确定具体的组件或其提供商，这是“实现系统”中的任务。

该阶段中的某些重要的 ISSE 事项包括：

- 系统组件要包含技术和非技术性机制（例如法律法规要求）。
- 系统安全设计必须符合面向客户的设计约束。
- 均衡取舍研究必须考虑到优先级、成本、进度、性能以及残余安全风险。
- 风险分析必须考虑到安全机制的互依赖性。
- 设计文档应当接受严格的配置控制。
- 系统安全设计应当能够追踪到安全要求。
- 系统安全设计应当考虑到长期工程项的进度和成本及对生命周期的支持。
- 系统安全设计应当包括修改过的安全 CONOPS。

在本阶段中，信息系统安全工程师还应当执行互依赖分析，比较安全机制的强度，审查所选择的安全服务和机制是否能够对抗 IPP 中列出的信息威胁。一旦该阶段完成，则风险评估的结果，尤其是风险的减缓需求以及残余风险，必须得到记录并通知给客户，得到客户的认同。

7.2.6 实现系统安全

“实现系统安全”的目标是采购、集成、配置、测试、记录和培训，它使系统从设计转入运行。该项活动的结束标志是最终系统的有效性评估行为，给出系统满足要求和任务需求的证据。其中，必须考虑到系统工程的主功能，解决好互依赖性和均衡取舍问题。

在该阶段，信息系统安全工程师需要——

- 验证系统的确能够防御此前的威胁评估中确定的威胁。
- 跟踪信息保护机制在系统实现和测试活动中的运用情况。
- 审查系统的生命周期计划、运行流程以及培训材料，并向这些文档提供输入。
- 实施正式的信息保护评估，为最终的系统有效性评估作出准备。

这些工作和信息均将对最终的系统有效性评估提供支持。

选择需要在解决方案中集成的具体安全产品是本阶段的工作任务之一。这些产品可通过购买、租用等多种选择来获得，影响选择的因素包括组件成本、可用性、形式以及适宜性。其它的因素包括系统组件的依赖性效果、组件的最低性能可能对系统性能的影响以及组件或替代品在将来的可用性。不能购买的组件必须自制。不论是软件、硬件还是固件，必须基于设计规范进行验证，并正式记录。必须评估所发现的任何偏差，检验这种偏差对设计实现和任务或业务目标的影响，包括对安全的影响。

无论选择购买还是自制，所有的组件必须按设计的要求集成到系统中，要解决与系统中既有组件的不兼容性。一个系统通常是既包含购买的组件，也包含自制组件的混合体，它们需要“粘合”，例如软件或接口电缆。在安装和配置过程中，需要的功能必须实现，而任务不需要的功能则必须予以限制。

信息系统安全工程师必须检验安全组件的评估准则，验证安全组件是否能满足这些准则。

ISSE 工程组可对组件的配置工作提供帮助，确保安全特性能够启动，且安全参数的配置能够使其提供所需的安全服务。一旦系统准备接受这些配置，则需要做出变更的设置必须得到记录，且应根据配置管理流程得到批准。

系统和设计工程师需要撰写测试流程，在其中反映出设计方案期望的结果。系统中需要的组件要进行单元测试。此外，所有的接口均需要测试。当然，如果系统比较特殊，或者运行在一个难以建模的环境中，则在系统建造完成前很可能无法全面测试所有接口。

集成测试将验证子系统或系统的性能。测试计划应考虑到单个组件以及整个系统测试所需的人员、

工具、设施、进度以及资金等问题。当组件集成到系统之中且对子系统和系统的功能作过测试后，其中的某些组件有可能需要作出变更。测试中发现的所有正面或负面结果均应得到记录。

系统的实现过程中，设计文档和经验是用户和管理员的培训资料来源。所有的文档应该接受严格的版本控制。培训材料和指南中应当讨论系统的运行策略，处理系统的限制以及系统功能。

在集成和测试时，重要的一项工作是记录下安装、操作、维护和支持的流程。这些流程将以系统要求、体系结构、设计和模型系统（按实际运行情况进行配置）的测试结果为基础。在安装系统时，必须记录下安装流程的不足，说明安装流程的变更会对功能和任务目标产生的影响。系统的运行、支持和维护过程中的残余风险可能因安装流程的变更而受到的影响也应得到评估。

信息系统安全工程师将负责制定信息保护测试计划和流程，可能还需要设计测试用例、工具、硬件和软件。该阶段的 ISSE 活动还包括——

- 参与保护机制和功能的测试。
- 在系统实现和测试过程中跟踪并应用信息保护机制。
- 审查系统生命周期的安全支持计划，包括后勤、维护和培训计划，并对这些计划提供输入。
- 持续实施风险管理。

信息系统安全工程师将监督系统接口、集成、配置，监督文档中的安全事项。系统测试和评估中可能会发现未知的脆弱性，必须评估这些脆弱性的风险及其对任务带来的可能影响。测试和评估结果需要不断反馈给设计工程师。信息系统安全工程师还要监督安全设计的正确实现。为此，信息系统安全工程师需要观测并参与测试过程，并分析测试和评估结果。

在该项活动中，要实施风险分析并制定风险减缓战略。信息系统安全工程师要标识出风险可能对任务带来的影响，并向客户提供建议。

信息系统安全工程师要确保所有文档已经完成并交付。文档中将包括有集成和测试报告，能够说明实际实现与设计规范之间的偏差。信息系统安全工程师可以参与撰写并审查这些文档。

ISSE 工程组要确保安全培训材料已经到位，且必须将运行中的威胁告知用户。在系统规范以及运行安全策略中要指明威胁信息和安全责任。

7.2.7 评估信息保护的有效性

“评估信息保护的有效性”活动跨越了整个 ISSE 过程。因此，上面每一小节均讨论到了该问题。表 7-1 概要描述了 ISSE 各项活动中的有效性评估任务。

表 7-1 ISSE 活动中评估信息保护的有效性任务

ISSE 活动	评估信息保护的有效性任务
发掘信息保护需求	● 概述信息模型。 ● 描述任务或业务的信息攻击威胁。 ● 得到客户对本阶段活动结论的认同，作为判断系统安全有效性的基础。
定义系统安全要求	● 确保所选择的解决方案集满足了任务或业务的安全需求。 ● 协调系统边界。 ● 向客户提供并展示安全背景环境、安全 CONOPS 以及系统安全要求，并获得客户的认同。 ● 确保预期的安全风险能被客户接受。
设计系统安全体系结构	● 开展正式的风险分析，确保所选择的安全机制能够提供所需的安全服务，并向客户解释安全体系结构如何满足安全要求。
开展详细的安全设计	● 执行互依赖分析，比较安全机制的强度，审查所选择的安全服务和机制是否能够对抗信息威胁。 ● 一旦完成设计，风险评估的结果，尤其是风险减缓需求和残余风险，需要得到记录并获得客户的认同。
实现系统安全	● 实施并更新风险分析。 ● 制定风险减缓战略。 ● 标识风险可能对任务带来的影响。

7.3 系统安全工程-能力成熟度模型（SSE-CMM）

7.3.1 概述

1. 目的

SSE-CMM 是系统安全工程—能力成熟度模型的简称，其确立了信息安全工程方面的基础标准，特别是满足了对信息安全工程过程能力的改进与评估的需要。无论是用户，还是信息安全提供商，都

希望安全产品、系统和服务能够得到不断的提高，尤其是通过信息安全工程的实施来达到该目的。此外，信息安全工程的实施过程对于各利益相关方来说都是可见的，这就更突出了可评估的信息安全工程方法的必要性。长久以来，安全工程领域已经先后产生了若干广为接受的方法（例如上节的 ISSE），但却一直缺少用来评估安全工程实施的框架。SSE-CMM 则弥补了这一缺憾，为信息安全工程方法的应用提供了一个衡量和不断改进的途径。

现代统计过程控制理论表明，通过强调生产过程的质量性和在这些过程中组织措施的成熟性，可以取得更为理想的成本效益。鉴于在开发安全系统和可信产品时所需的成本和时间不断增加，客观上就需要有更加高效的工程过程。安全系统的运行和维护也依赖于同人员和技术相互紧密联系的工程过程。通过强调过程的质量及这些过程中的组织措施的成熟性，可以以更好的成本效益来管理信息安全工程过程中各类元素之间的互依赖性。

SSE-CMM 项目的目标是发展一个得到良好定义的、成熟的且可度量的信息系统安全工程方法。使得如下工作成为可能：

- 使安全工程组织把安全投资更有效地集中在安全工程工具、培训、过程定义、管理措施以及改进上；
- 提供基于能力的保证，即基于对工程组织的安全措施和过程的成熟性的信心而达到必要的信任度（即保证）；
- 通过区分投标者的能力级别和相关的项目风险来选择合格的安全工程提供商。

2．历史

SSE-CMM 的基础是 CMM（能力成熟度模型）。CMM 的 1.0 版本在 1991 年 8 月由卡内基-梅隆大学软件工程研究所（SEI）发布，在多次讨论和修订后成为软件界用来评审软件开发工程的业界标准。意识到 CMM 对工程过程能力的重要意义后，美国国家安全局在研究信息安全工程能力评价准则时便选取了 CMM 的思想作为其方法学。SSE-CMM 的研究项目自 1993 年启动，1996 年 10 月发布了 SSE-CMM 的 1.0 版本，1999 年 4 最终形成了 SSE-CMM 的 2.0 版本，2003 年 6 月由国际系统安全工程协会（ISSEA）更新为 3.0 版本。不同于 ISSE，它是包括军方在内的社会各方面合作的结果，其应用不再局限于指导军方的信息安全工程实践，而是通过对信息安全工程能力成熟度的标准性、公开化评估获得安全保证。因此，SSE-CMM 字诞生后产生了比较广泛的影响，并在 2002 年成为国际标准 ISO/IEC 21827: 2002《信息技术 系统安全工程 能力成熟度模型》。2008 年 10 月，国际标准化组织基于 SSE-CMM 3.0 发布了 ISO/IEC 21827: 2008。

经对 ISO/IEC 21827: 2002 转化后，我国于 2006 年发布了国家标准 GB/T 20261-2006《信息技术 系统安全工程 能力成熟度模型》。此外，我国信息安全等级保护工作中，也充分吸收了 SSE-CMM 的内容，制定了国家标准 GB/T 20282-2006《信息安全技术 信息系统安全工程管理要求》。

3．SSE-CMM 的范围

SSE-CMM 的范围包括：

- SSE-CMM 涉及到可信产品或者安全系统的整个生命周期内的安全工程活动，包括了概念定义、需求分析、设计、开发、集成、安装、运行、维护和终止；
- SSE-CMM 可应用于安全产品开发商、安全系统开发商和集成商，以及提供安全服务和安全工程的组织；
- SSE-CMM 可应用于所有类型和大小的安全工程组织，例如商业组织、政府组织和学术组织。

虽然 SSE-CMM 是一个清晰的信息安全工程模型，但这并不意味着 SSE-CMM 与其它工程方法是相隔离的。相反，SSE-CMM 充分认识到，信息安全需要综合所有可行的工程过程，例如系统、软件、硬件和人为因素。因此，SSE-CMM 是开放性的，可以向其中不断添加新的安全工程过程及其它相关的过程。

7.3.2 SSE-CMM 的体系结构

SSE-CMM 体系结构是其方法学的核心。这个体系结构的目标是清晰地从管理和制度化特征中分离出安全工程的基本特征，因此该体系结构被设计成可在整个安全工程范围内决定安全工程组织的过

程成熟性。为了保证上述的分离，SSE-CMM 模型是两维的，分别称为“域”和“能力”。

需要特别强调的是，SSE-CMM 并不意味着在一个组织中的工程项目组必须去实施这个模型中所描述的全部过程，也不要求使用最新和最好的安全工程技术及方法。然而，SSE-CMM 模型必须要求的是，一个组织一定要有一个包括了 SSE-CMM 中所描述的“基本安全实施”的工程过程。此外，一个组织还可以以任何方式随意创建满足其业务目标的过程和组织结构。

1．基本模型

SSE-CMM 中包括两维：“域”和“能力”。域维是这两个维中较易理解的。这一维由所有定义安全工程的工程实施活动组成。这些实施称为“基本实施”（Base Practice）——BP。

能力维也由一系列的工程实施活动组成，但这些工程实施活动代表的是组织对过程的管理和制度化能力。它们称作“通用实施”（Generic Practice）——GP，通用实施是基本实施过程中必须完成的活动。

图 7-5 中举例描述了基本实施和通用实施之间的关系。该图说明如下：

某一安全工程组织正在实施“标识系统安全脆弱性”的活动，这是一种基本实施过程，在 SSE-CMM 中编号为 05.02。

那么，在判断该组织实施这一活动的能力时，考察方面之一就是察看其是否为这一活动分配了资源，这是在通用实施列表的“分配资源”中要求。

于是，通过把基本实施和通用实施在两个维上综合考察，便可以评估一个组织实施特定的安全工程过程的能力。图 7-5 可以回答客户这样的提问：“你的组织在查找系统安全脆弱性时，是否具备必要的资源？”根据其回答，该客户便可得知这一工程组织在工程实施资源方面的工程能力。

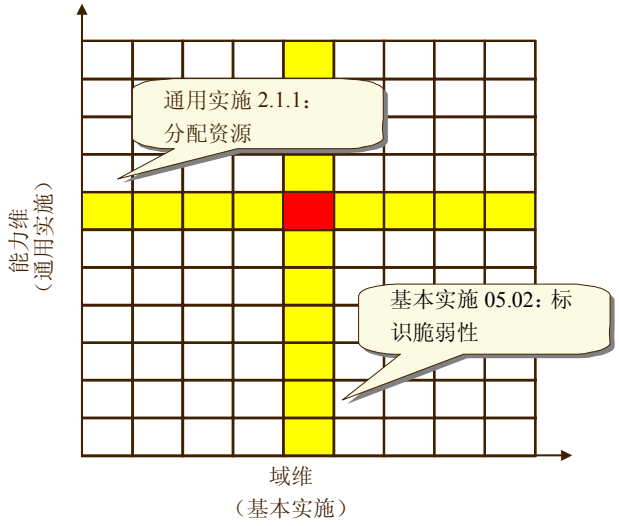


图 7-5　举例说明通用实施与基本实施之间的关系

在回答了所有交叉点的问题之后，客户便可获知一个安全工程组织的总体工程能力。

2．基本实施及过程域

SSE-CMM 包含了 61 个基本实施过程，这 61 个基本实施被归入了 11 个安全工程过程域（Process Area，简称 PA），它们覆盖了安全工程主要领域。基本实施来源于大量的文献材料、实践经验以及专家知识。一般来说，这些基本实施的选择代表了安全工程界最为优秀的安全工程过程实施活动，所有的活动都得到了实践的验证。

确定这些基本实施的内容是很复杂的一项工作。最大的困难在于，成熟的实施过程很多，而由于历史的原因，其中有大量名称不同但实质内容相同的实施过程。而且，这些过程在系统生命周期中的出现阶段、抽象程度、执行角色各不相同。SSE-CMM 避开了这些差异，选取的均是对安全工程来说非常根本和重要的过程实施行为。

这些基本实施应该满足：

- 应用于企业的整个生命周期；

- 与其它的 BP 不相互覆盖；
- 代表了安全界的“最好的实施”；
- 不能只简单地反映最新技术；
- 可在多种业务环境下以多种方法运用；
- 不指定具体的方法或工具。

在将 61 个基本实施划归为 11 个过程域（PA）时，可供选择的方法很多。方法之一是为真实世界建模，创建能匹配实际的安全工程服务的过程域。最终，在确定现有的 11 个 PA 时，SSE-CMM 综合了这些方法的优势。每一个过程域内的基本实施都有一个共同的关注焦点，能够达到一套清晰的安全工程目标。

一个过程域应该：

- 汇集一个域中的相关活动，易于使用；
- 与有价值的安全工程服务相联系；
- 可应用于组织的整个生命周期；
- 能在多个组织和多种产品背景下实施；
- 能作为一个独立的过程加以改进；
- 能够被有类似兴趣的工程组加以改进；
- 包括了能满足该过程域目标的所有 BP。

图 7-6 说明了域维中过程域与基本实施的关系。

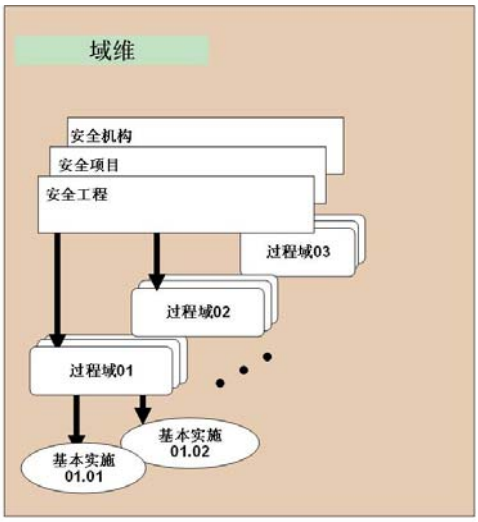


图 7-6　域维中过程域与基本实施的关系

SSE-CMM 的 11 个过程域列举如下。需要注意的是，这些 PA 是以字母顺序排列的，而非按照生命周期的顺序排列。

- PA01 管理安全控制
- PA02 评估影响
- PA03 评估安全风险
- PA04 评估威胁
- PA05 评估脆弱性
- PA06 建立安全论据
- PA07 协调安全
- PA08 监视安全态势
- PA09 提供安全输入
- PA10 确定安全需求
- PA11 验证与确认安全

除如上的过程域外，SSE-CMM 还包括了与工程项目和组织措施相关的其它 11 类过程域，它们来自于系统工程能力成熟度模型（SE-CMM）。如下所列：

- PA12 确保质量
- PA13 管理配置
- PA14 管理项目风险
- PA15 监视和控制技术工作
- PA16 规划技术工作
- PA17 定义组织的系统工程过程
- PA18 改进组织的系统工程过程
- PA19 管理产品线发展
- PA20 管理系统工程支撑环境
- PA21 提供不断发展的技能和知识
- PA22 与提供商相协调

这些过程域并不是与安全工程直接相关的，但它们也会对安全工程造成影响。因此也常常受到安全工程组织的重视。

3．通用实施与公共特征

通用实施是应用于所有过程域中的活动。它们针对的是过程的管理、测量和制度化。它们将应用于 SSE-CMM 的评定活动之中，用以判断一个组织完成某个基本过程的能力。

如同基本实施被归为 11 类过程域一样，通用实施也被归入了 12 个不同的逻辑域，称为“公共特征”（Common Feature）。这 12 个公共特征被分为五个能力级别，代表了依次增长的安全工程能力。但它与域维中的基本实施所不同的是，能力维中的通用实施是按成熟度排序的，因而代表高级实施能力的通用实施位于能力维的高端。

公共特征目的旨在描述一个组织实施安全过程的能力。每一个公共特征包括一个或多个通用实施。最低的公共特征为“1.1 执行基本实施”，该级的通用实施只是检查一个组织是否实现了某个过程域中的所有基本实施。

后续公共特征中的通用实施将可以用来判断工程项目是如何管理和改进每一个过程域中基本实施的实现情况的。表 7-2 描述了通用实施所秉持的主要原则。

表 7-2　能力维的原则

原则	如何在 SSE-CMM 中表述
在管理一个对象之前，必须首先实现该对象	非正式实施级将关注一个组织是否实现了基本实施中的工程过程
在定义组织层面的过程之前要理解项目的全部信息（例如该项目的产物是什么）	计划和跟踪级将关注项目层面的定义、规划和实施事项
使用从项目中学到的最佳知识来创建组织层面的过程	充分定义级将关注对在组织层面上定义的过程进行（融合了多个专业领域知识的）裁剪
只有清晰了解了一个对象，才能测量该对象	在计划和跟踪级，对安全工程项目进行基本的测量是很重要的，但直到充分定义级，SSE-CMM 才开始注意在组织层面上搜集测量数据，直到量化控制级，全面的项目测量成为可能
只有测量了正确的对象，基于测量的管理才有意义	量化控制级将关注对组织业务目标的测量
一个持续改进的文化必须以良好的管理措施、既定过程、可测量的目标为基础	持续改进级将通过以前的能力级获得最大可能的收益，强调文化的形成，以保持这种收益

下面各个级别中的公共特征表示了为获得每一个级别的成熟度而需要满足的安全工程属性。

- 能力级 1
  - 1.1 执行基本实施
- 能力级 2
  - 2.1 规划执行
  - 2.2 规范化执行
  - 2.3 验证执行
  - 2.4 跟踪执行
- 能力级 3

- 3.1 定义标准过程
- 3.2 执行既定的过程
- 3.3 协调过程

- 能力级 4
  - 4.1 建立可测量的质量目标
  - 4.2 客观地管理执行
- 能力级 5
  - 5.1 改进组织的能力
  - 5.2 改进过程的有效性

图 7-7 说明了能力维中公共特征与通用实施之间的关系。

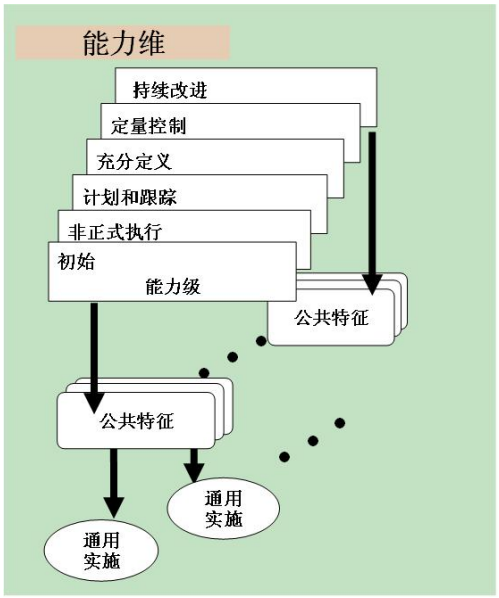


图 7-7　能力维中公共特征与通用实施之间的关系

4．能力级别

人们从长期的工程实践中发现，有很多方法可以将实施活动根据公共特征进行分类，也有很多不同的方法可以将公共特征划分到多个能力级别之中。因此，在介绍 SSE-CMM 能力级别时，仍有必要进一步深入说明 SSE-CMM 的公共特征。

之所以有公共特征的排序问题，是因为某个级别安全过程的实施和制度化要建立在其它级别实施和制度化的基础之上。在一个组织能够有效地定义、裁剪和使用一个过程之前，工程项目组必须具有管理这些工程绩效的经验。例如，一个组织首先应该对一个项目进行评价，然后才能为整个组织的评价过程进行规范。当然，在有些方面，当过程的实施和制度化应放在一起考虑以提高工程能力时，可以不考虑前后次序。

无论是评估还是改进一个组织的过程能力，公共特征和能力级别都是很重要的。在评估一个组织的工程能力时，如果该组织只是执行了一个特定级别的部分公共特征，而非全部，则该组织对这个过程而言，应处于这个级别的最低层。例如，在第 2 级能力上，如果缺乏跟踪执行这一公共特征的经验和能力，那么跟踪项目的执行将会非常困难。如果高级别的公共特征在一个组织中得到了实施，而某些低级别的公共特征却未能实施，那么这个组织也不能获得该级别的所有好处。

当一个组织希望通过 SSE-CMM 改进其过程能力时，该组织可以依次执行各级别中的通用实施行为，相当于 SSE-CMM 为组织提供了“能力改进路线图”。因此，SSE-CMM 的实施应按公共特征进行组织，并按级别进行排序。

在判断每一个过程域的能力级别时，均需执行评估过程。若需要评估一个组织在多个过程域上的能力级别，则必须执行多次评估过程。这意味着，同一个组织可能在不同的过程域上会有不同的能力

级别。因此，在该组织准备改进其能力级别时，它便可以首先侧重于在级别相对较低的过程域内提高其能力，这种优先级对于组织的能力改进工作来说是很有意义的。

通用实施、公共特征、能力级别的关系如图 7-8 所示。

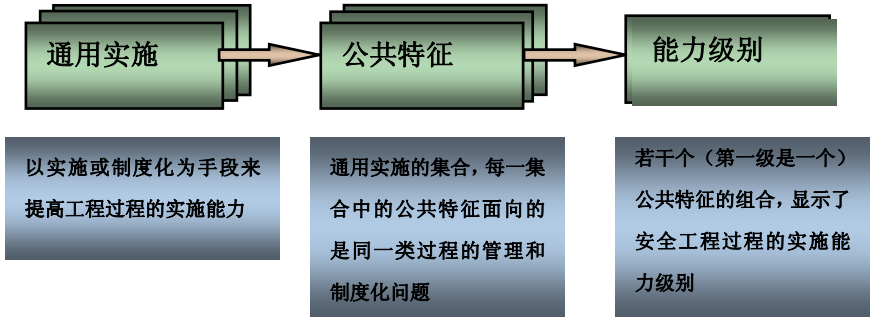


图 7-8　通用实施、公共特征、能力级别的关系

SSE-CMM 包含五个能力级别（此外还有第 0 级，表示无安全功能能力，故一般不予讨论）。这五个级别的概述如下。

- 1 级：“非正式执行级”，该级将关注一个组织或项目是否执行了包含基本实施过程的安全工程。该级别的特点可以描述为“你必须首先做它，然后才能管理它”。
- 2 级：“计划和跟踪级”，该级将关注项目层面的定义、规划和执行问题。该级别的特点可描述为“在定义组织层面的过程之前，先要理解项目的相关事项”。
- 3 级：“充分定义级”，该级将关注于在组织层面上从既定过程中实施已融合了各个专业领域知识的裁剪。该级别的特点可描述为“用项目中学到的最好的东西来创建组织层面的过程”。
- 4 级：“量化控制级”，该级将关注于测量，它是与组织的业务目标紧密联系在一起的。这个级别的特点可以描述为“只有你知道它是什么，你才能测量它”以及“当你测量正确的对象时，基于测量的管理才有意义”。
- 5 级：“持续改进级”，该级将从此前各级的所有管理活动中获得最大的收益，并强调组织的文化，以保持所取得的成果。该级别的特点可以描述为“一个持续改进的文化需要以良好的管理措施、既定过程和可测量的目标为基础”。

图 7-9 显示了 SSE-CMM 的 5 个能力级别及其包含的公共特征。

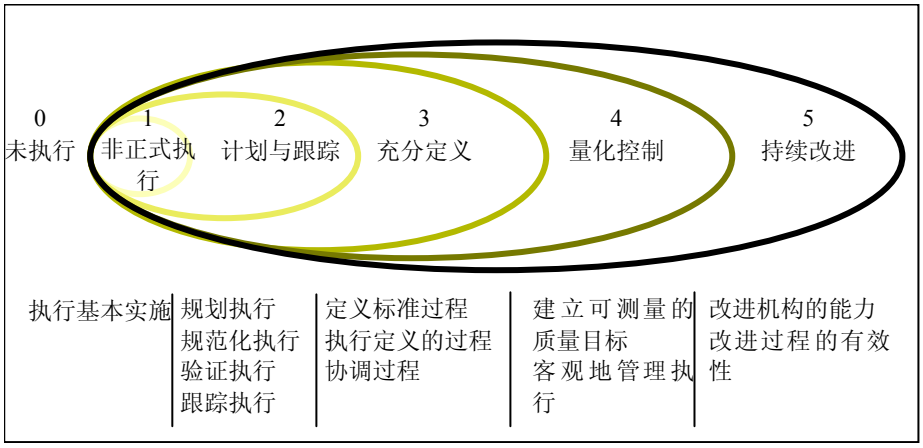


图 7-9　SSE-CMM 的 5 个能力级别及其包含的公共特征

7.3.3　安全工程的过程分类

SSE-CMM 不是基于时间维描述信息安全工程过程的，而是将通用的安全工程过程分为了若干个不同的单元域。这样做必然会导致一个问题：安全工程过程的分类有无逻辑可循？

SSE-CMM 在该问题上的处理很有条理，它将安全工程过程划分为三个基本的过程域组：风险、工程、保证。这三个基本的过程域组便是 SSE-CMM 观察安全时的主要焦点。虽然它们之间绝不是互相独立的，但可以对它们单独地加以考虑。这三者关系最为简单的体现如下：风险过程将标识出所开

发的产品或系统中存在的危险并对这些危险进行优先级排序；针对危险所可能导致的问题，安全工程过程要与其它工程方法一起合作，确定并实施解决方案；最后，安全保证过程将为解决方案建立起信任度，并将这种信任度转达给客户。

图 7-10 显示了 SSE-CMM 中安全工程过程的三个主要部分。

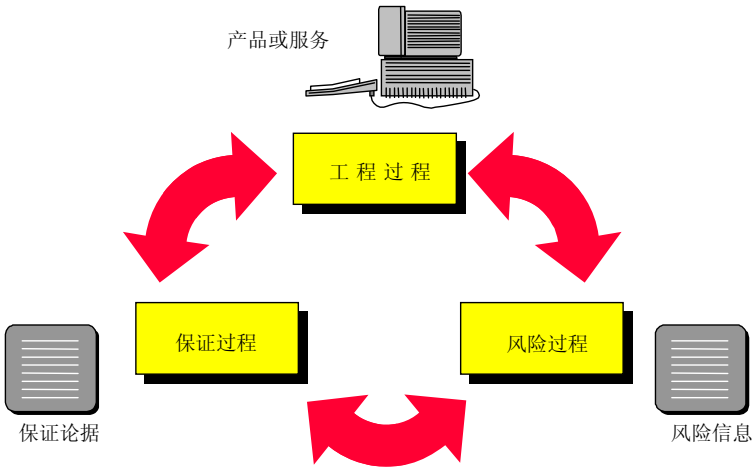


图 7-10　安全工程过程的三个主要部分

在上述三个部分的联合下，便可达到 SSE-CMM 所提出的安全目标。

以下将分别分析其三类过程的主要内容。

1．风险

安全工程的一个主要目标是减缓风险。风险评估就是确定尚未发生的潜在问题的一种过程。风险要通过检查威胁和脆弱性发生的可能性、考虑安全事件的潜在后果来进行评估。一般来说，可能性中必然含有不确定因素，而一个不确定因素要依赖于具体情况。这就意味着，这种可能性只可能在某种限制条件下进行预测。此外，对安全事件影响的评估也要涉及到不确定因素。总而言之，这些评估对象中含有大量的不确定性因素，因而对安全的规划和判断将变得非常困难。

一个有害事件总由三个部分组成：威胁、脆弱性和影响。脆弱性是资产本身的属性，相当于矛盾论中的内因，它常被威胁利用来实施攻击（威胁因而也被称为矛盾论中的外因）。此外，脆弱性也包括资产中存在的弱点和不足。威胁和脆弱性中，只要任何一个不存在，就不会发生有害事件，也就不存在风险。风险管理是评估和量化风险、并建立起组织对风险的承受级的过程。它是安全管理的一个重要组成部分。

图 7-11 说明了风险评估涉及的内容及 SSE-CMM 中与此有关的过程。

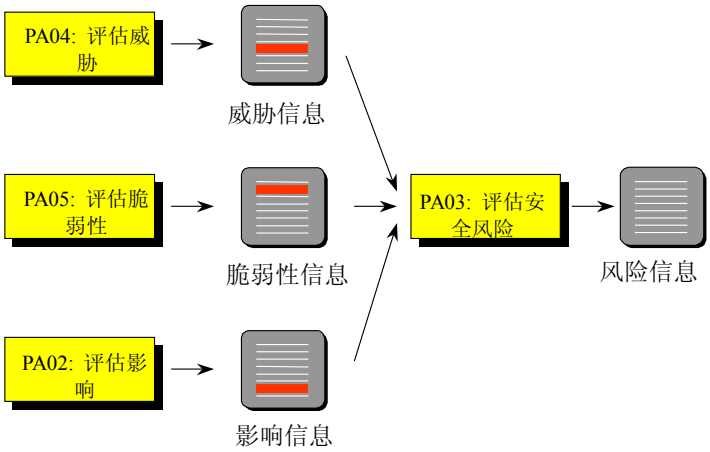


图 7-11　SSE-CMM 中与风险过程相关的过程域

为了减缓风险，需要实施安全措施。安全措施可针对威胁、脆弱性、影响或风险自身。但无论如何，安全措施并不适合于减缓所有风险，或彻底根除某个具体风险。这主要是因为风险减缓所需的代

价和相关的不确定性造成的，所以某些残余风险必须接受。在不确定性很高的情况下，由于风险的不精确特性，判断是否接受风险便成为一个非常专业的问题。图 7-10 中的几个 SSE-CMM 过程域可用来分析组织的威胁、脆弱性、影响及相关的风险。

除上述的风险减缓和风险接受外，还存在其它两类风险处理方法：风险规避与风险转嫁。前者指不介入风险，例如拆除信息系统；后者指通过某种手段（例如签订协议），将安全风险转嫁给其他方承担，例如与保险公司签订协议，将组织的信息安全投保。

2．工程

这是信息安全工程中必不可少的内容。虽然 SSE-CMM 没有按照时间顺序阐述安全工程过程，但仍在“工程”部分中涵盖了工程的各个阶段，这体现了对 ISSE 的继承。SSE-CMM 理解的安全工程仍然是周期性的，包括了概念、设计、实施、测试、部署、运行、维护、终止。在此之中，安全工程师必须与其它的系统工程组密切合作。SSE-CMM 强调，安全工程师是一个大的项目组中的一部分，需要与其它领域的工程师的活动相互协调。这有助于确保安全成为一个大的项目过程中的一个合成部分，而不是一个独立的、不相干的活动。

应用从“风险”部分得来的信息以及关于系统需求、相关法律、政策的其它信息，安全工程师就可以与客户合作，一起来确定安全需求。然后，安全工程师便可进一步确定并跟踪特定的安全需求。

图 7-12 说明了 SSE-CMM 中与工程相关的过程域。

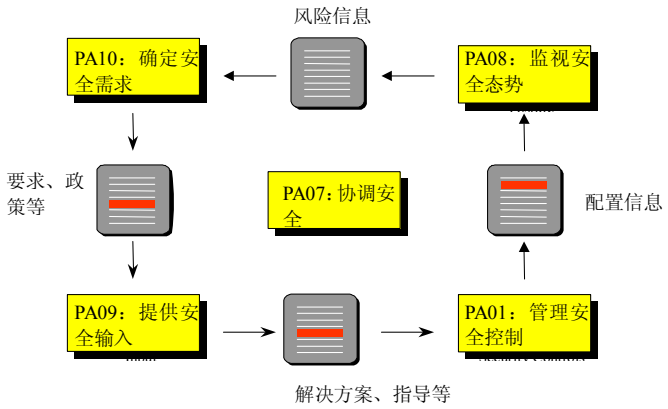


图 7-12　SSE-CMM 中与工程过程相关的过程域

一般来说，创建安全问题的解决方案过程涉及到标识所有可能的备选方案，并从中确定哪一种更加适合。这其中的难度在于，选择这些解决方案时不能只考虑安全问题。除安全问题外，还需要考虑大量的其它因素，其中，成本、性能、技术风险、易用性等因素必须考虑。这些分析的结果也为 SSE-CMM 的第三大焦点——保证——提供了意义重大的基础。

在生命周期的后期，安全工程师应确保产品和系统已经得到了正确的配置，可以对付已知的风险，并确保新风险不会造成系统运行的不安全。

3．保证

SSE-CMM 认为，保证是安全工程中非常重要的成果。当前存在着很多种保证方法，SSE-CMM 的信任程度（即保证）来自于安全工程过程结果的可重复性。这种信任度的基点是：成熟组织比不成熟组织更有可能产生可重复的工程结果。

需要指出，安全保证并不能添加任何额外安全风险控制措施，但它能为安全控制措施可减少预计的安全风险提供信心。

图 7-13 说明了 SSE-CMM 中与保证相关的过程域。

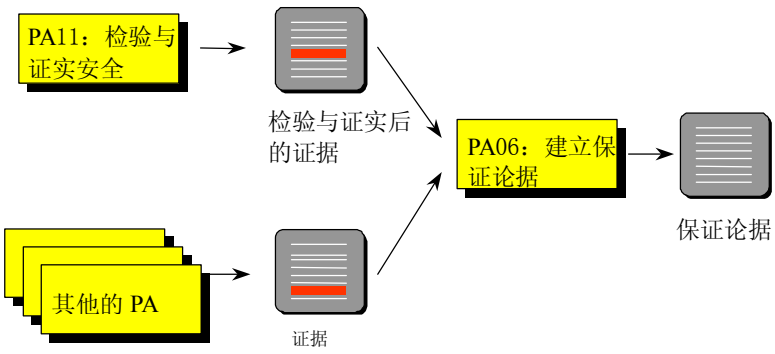


图 7-13　SSE-CMM 中与保证过程相关的过程域

安全保证也可看作是安全措施按照预期目标运行的信心。这种信心来自于安全措施的正确性和有效性。正确性保证了安全措施设计实现了需求。有效性则保证了所提供的安全措施可充分地满足客户的安全需要。安全机制的强度也会对这种信息起作用，但要受到保护级别和所追求的保障程度的制约。

安全保证通常以论据的形式在 SSE-CMM 的各个过程之间交流。论据包含了对系统属性的声明集。这些声明都要有相关证据来支持。一般说来，这些证据都是以文档的形式存在，文档则常常在安全工程活动期间就得到了开发。

SSE-CMM 活动本身涉及到了相关保证证据的产生。例如，过程文档能够说明开发遵循了一个得到充分定义的、成熟的、不断改进的工程过程。对安全效果的验证与确认则用来建立一个可信产品或系统的可信度。

此外，在过程域中还有很多典型工作结果可作为证据或证据的一部分。现代统计过程控制表明，通过注重产品的生产过程，则能够以较好的成本效益比重复地生产出高质量、高保证的产品。一个组织的组织措施的成熟度将会影响到这些过程。

本章小结

本章介绍了信息安全工程的基本原理和有关国际标准的主要要求。

本章内容主要有：

（1）系统工程过程

系统工程过程是信息系统安全工程的基础。常见的工程过程一般有以下几个部分：挖掘任务或业务需求、定义系统功能、设计系统、实施系统、评估有效性。

在挖掘任务或业务需求阶段，主要的工程行为是描述任务/业务并考虑有关的政策要求。在定义系统功能阶段，系统工程师要明确系统的目标，定义系统背景/环境，将目标转化为系统功能和性能要求，并进行功能分析，要点是分析功能之间或功能与环境之间的联系。在设计系统阶段，系统工程师要完成功能分配、概要设计和详细设计工作。在实现系统阶段，系统工程师要完成采购、建设和测试任务。最后，系统工程师要从系统是否达到了任务需求以及系统是否能够依照组织所期望的方式操作这两方面来评估系统的有效性。

（2）信息系统安全工程（ISSE）过程

信息系统安全工程是美国军方在系统工程过程的基本原理基础上开发的信息安全工程方法学，其重点是通过实施系统工程过程来满足信息保护的需求。ISSE 有三个主要原则：（a）始终将问题空间和解决方案空间相分离。（b）问题空间要根据客户的任务或业务需求来定义。（c）解决方案空间要由问题空间相驱动，并由系统工程师和信息系统安全工程师来定义。

信息系统安全工程过程与系统工程过程类似，其主要阶段包括发掘信息保护需求、定义信息系统安全要求、设计系统安全体系结构、开展详细的安全设计、实现系统安全以及评估信息保护的有效性。

（3）系统安全工程-能力成熟度模型（SSE-CMM）

SSE-CMM 是在 CMM（能力成熟度模型）原理基础上发展起来的，可用于对信息安全工程过程能力进行改进与评估的重要标准。SSE-CMM 的目标是清晰地从管理和制度化特征中分离出安全工程的

基本特征，因此其体系结构被设计成可在整个安全工程范围内决定安全工程组织的过程成熟性。为了保证上述的分离，SSE-CMM 模型是两维的，分别称为“域”和“能力”。维由所有定义安全工程的工程实施活动组成，分别与风险、工程、保证相关，称为“基本实施”；能力维也由一系列的工程实施活动组成，但这些工程实施活动代表的是组织对过程的管理和制度化能力称作“通用实施”，是基本实施过程中必须完成的活动。SSE-CMM 包含五个能力级别分别是 1 级“非正式执行级”、2 级“计划和跟踪级”、3 级“充分定义级”、4 级“量化控制级”、5 级“持续改进级”。

习题

1．系统工程过程由哪些部分组成？
2．信息系统安全工程过程由哪些部分组成？
3．信息系统安全工程过程的三个主要原则是什么？
4．发掘信息保护要求与定义系统安全要求之间的关系是什么？
5．概述定义系统要求与设计系统体系结构的区别。
6．概述 SSE-CMM 的基本模型。
7．SSE-CMM 中，域维和能力维的区别是什么？
8．SSE-CMM 规定了几个能力级别？
9．概述 SSE-CMM 中通用实施、公共特征和能力级别的关系。

第 8 章　信息安全管理

本章要点

- 信息安全管理的重要性
- 与信息安全管理有关的主要标准
- 信息安全管理控制措施
- 建立信息安全管理体系（ISMS）的过程
- 信息安全风险评估主要过程

8.1　概述

信息安全管理是信息安全中的重要概念，信息安全管理控制措施是与信息安全技术控制措施一起构成了信息安全防护措施的全部。因此，我国将“管理与技术并重”作为信息安全保障的一项基本原则。近年来，国际和国内标准化组织大力加强信息安全管理标准的制定，在很大程度上推动了信息安全管理的研究与应用。

8.1.1　什么是管理和信息安全管理

什么叫管理?许多管理学者从各自不同的角度下过不同的定义。有的说，管理就是管人；有的说，管理就是决策；有的认为，管理是通过他人将事情办成功的艺术；有的认为，管理是为了实现预定目标，组织和使用各种资源的过程。马克思没有直接对管理下过定义，但有一段话谈到了管理的必要性。他说：“一切规模较大的直接社会劳动或共同劳动，都或多或少地需要指挥，以协调个人的活动。”这里提到的“指挥”和“协调”，都属于管理范畴。紧接着他打了一个比喻：“一个单独的提琴手，是自己指挥自己；一个乐队，就需要一个乐队指挥。” 这个比喻，生动地说明个人活动与群体活动的最大区别是前者不需要别人指挥，后者则需要管理。因此，管理学中的“管理”定义可以这样理解：凡是有群体共同活动、共同劳动或共同工作的地方，都需要管理。管理是管理人员领导和组织人们去完成一定的任务和实现共同的目标的一种活动。“管理”有这样几个特点：“人”是管理的主体；管理要以规章制度为手段，管理对象必须遵从这些规章制度；管理离不开事先的组织、规划以及实施过程中的协调。

毫无疑问的是，任何一种管理活动都必须明确谁来管（即管理主体）、管什么（即管理客体）、怎么管（即管理手段）以及管得怎么样（管理效果）的问题。

“管理”的概念应用到信息安全领域，便有了信息安全管理的概念。美国的国家标准与技术研究院（NIST）将信息安全技术控制措施定义为完全由机器来完成的活动，信息安全管理措施定义为完全由人来完成的活动，并将由机器和人共同完成的活动定义成信息安全运行控制措施。事实上，后两种都是信息安全管理控制措施。简言之，信息安全管理是指把分散的信息安全技术因素和人的因素，通过策略、规则协调整合成为一体，服务于信息安全的目标。

根据管理主体、管理对象等要素的不同，信息安全管理分为两个层次：

一是国家层次的信息安全管理。其管理的主体是代表国家意志的信息安全相关行政主管部门和技术主管部门，这些部门依法行使本部门对信息安全的管理职责，以战略方针、政策、法规、标准和其它措施为基本手段，重在创造良好的信息化和信息安全政策环境，合理划分

安全管理责任，有效分配国家和社会资源，积极调整各方关系，加强信息安全技术组织与建设，从宏观和全局角度推动信息安全保障体系中各项工作的落实。

另一种则是组织层面的信息安全管理。其管理的主体是一个组织的管理层和技术层，管理的对象是“人”和“技术”，管理的核心目标是建立组织内的信息安全管理体系，控制信息安全风险。其基本任务分为两个方面：通过信息安全管理过程完成信息安全在管理方面的要求；通过信息安全管理过程驱动信息安全技术的实施，达成信息安全在技术方面的要求。这一层次的信息安全管理带有微观性，但却涵盖了一个组织的全部信息安全工作。

由于信息化有通过网络互连、互通、互操作的特点，没有强力度的全局安全管理，仅靠局部是难以发挥信息化应有的效率和效益。而国际化的特点更需要有反映国家意志的国际交往原则和处理应对措施。因此，宏观信息安全管理是信息化社会有序健康运作的保证，是技术发展的推动力，是把分散的信息保障能力由“指头”变成“拳头”的聚合剂。另一方面，由于现代信息系统是人机结合的复杂系统，没有细粒度的对人和技术的有效安全管理，则系统的效率和效益难以发挥。因此，微观信息安全管理是人如何操作技术的规范尺度，是发挥人的因素和技术因素的桥梁。

宏观管理是对微观管理的指导和约束，微观管理是对宏观管理的贯彻和落实，二者紧密相关，互为依托，缺一不可。

8.1.2 信息安全管理的重要性

长期以来，人们保障信息安全的手段偏重于依靠技术，从早期的加密技术、数据备份、病毒防护到近期网络环境下的防火墙、入侵检测和身份认证等。厂商在安全技术和产品的研发上不遗余力，新的技术和产品不断涌现；消费者也更加相信安全产品，把大部分安全预算也都投入到信息安全产品的采购上。但事实上，仅仅依靠技术和产品保障信息安全的愿望却往往难尽人意，很多复杂、多变的安全威胁和隐患仅靠产品是无法消除的。此外，复杂的信息安全技术和产品往往在完善的管理下才能发挥作用。因此，人们在信息安全领域总结出了“三分技术，七分管理”的实践经验和原则。

对实际发生的信息安全事件的统计也凸显了信息安全管理因素的重要性。据有关部门统计，在所有的计算机安全事件中，约有 52%是人为因素造成的，25%由火灾、水灾等自然灾害引起，技术错误占 10%，组织内部人员作案占 10%，仅有 3%左右是由外部不法人员攻击造成的。简单归类，属于管理方面的原因比重高达 70%以上，而这些安全问题中的 95%是可以通过科学的信息安全管理来避免的。因此，信息安全管理已成为信息安全保障能力的重要基础。

如果说安全技术是信息安全的构筑材料，那么安全管理就是信息安全的粘合剂和催化剂，只有将有效的安全管理从始至终贯彻落实于安全建设的方方面面，信息安全的长期性和稳定性才能有所保证。信息安全管理一般包括制定信息安全政策、风险评估、控制目标与方式选择、制定规范的操作流程、对员工进行安全意识培训等一系列工作，通过在安全方针策略、组织安全、资产分类与控制、人员安全、物理与环境安全、通信与操作安全、访问控制、系统开发与维护、业务持续性管理、符合法律法规要求等若干个领域内建立管理控制措施，为组织建立起一张完备的信息安全“保护网”，保证组织信息资产的安全与业务的连续性。

8.1.3 国外信息安全管理相关标准

信息安全技术的发展极大地促进了信息安全管理理念的产生和发展，各种有关信息安全管理的法规、标准也应运而生。20 世纪 80 年代末，随着 ISO 9000 质量管理体系标准的出现及其随后在全世界的广泛推广应用，系统管理的思想在信息安全管理领域也得到借鉴与采用，使信息安全管理在 20 世纪 90 年代步入了标准化与系统化管理的时代。1995 年，英国率先推出了 BS 7799 信息安全管理标准，并于 2000 年被国际标准化组织批准为国际标准 ISO/IEC 17799 标准。澳大利亚和新西兰也联合推出了风险管理标准 AS/NZS 4360，德国的

联邦技术安全局推出了《信息技术基线保护手册》等。下面介绍几种主要的信息安全管理相关标准。

1．BS 7799 标准

BS 7799 是由英国标准协会（简称 BSI）制定的信息安全管理体系标准，它为保障信息的保密性、完整性和可用性提供了典范。虽然 BS 7799 是英国标准，但出版后得到了各国的认可，并得到了广泛的应用。BS 7799 包括两部分，BS 7799-1:1999《信息安全管理使用规则》和 BS 7799-2:2002《信息安全管理体系规范》，标准的第一部分为第二部分的具体实施提供了指南。BS 7799 广泛地涵盖了所有的信息安全议题，如安全方针的制定、安全责任的归属、风险的评估、访问控制，甚至包含防病毒的相关策略等。BS 7799 推出后很快成为国际公认的信息安全实施标准，适用于各种产业与组织。从 2000 年到 2005 年间，全球将近 2000 家组织获得了 BS 7799-2 的认证，在中国有将近 20 家单位获得了此认证。

BS 7799-1 是组织建立并实施信息安全管理的一个指导性的准则，主要为组织制订信息安全策略和进行有效的信息安全控制提供一个通用的方案，从而推动在组织内部实施和维护信息安全。BS 7799-1 从安全政策、组织安全、资产分类与控制、人员安全、物理与环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性管理、符合性管理等 10 个方面定义了 127 项控制措施。这其中，除了访问控制、系统开发与维护、通信与操作管理 3 个方面跟信息安全技术关系紧密以外，其它 7 个方面更侧重于组织整体的管理和运营操作。

BS 7799-2:2002 于 2002 年 9 月 5 日在英国发布。此版本在介绍信息安全管理体系的建立、实施和改进的过程中引用了 PDCA 模型，按照 PDCA 模型的信息安全管理体系分解成风险评估、安全设计与执行、安全管理和再评估 4 个子过程。BS 7799-2:2002 提出了建立信息安全管理体系的步骤，包括定义信息安全政策、定义 ISMS 的范围、进行信息安全风险评估、信息安全风险管理、确定控制目标和选择控制措施、准备信息安全适用性声明。

BS7799 标准之所以能被广为接受，一方面是它提供了一套普遍适用且行之有效的全面的安全控制措施，而更重要的，还在于它提出了建立信息安全管理体系的目标。与以往以技术为主的安全体系不同，BS 7799-2 提出的信息安全管理体系是一个系统化、程序化和文档化的管理体系，这其中，技术措施只是作为依据安全需求有选择、有侧重地实施安全目标的手段而已。

2．ISO/IEC 17799 标准

2000 年 12 月，BS 7799-1《信息安全管理实用规则》被国际标准化组织（ISO）正式批准成为国际标准，编号为 ISO/IEC 17799。此后，已有二十多个国家引用 ISO/IEC 17799 作为国家标准，ISO/IEC 17799 也一度成为卖出拷贝最多的管理标准，越来越多的信息安全公司都以 ISO/IEC 17799 做指导为客户提供信息安全咨询服务。ISO/IEC 17799 的最新版本是 ISO/IEC 17799:2005，新版本较早期版本做了一定的修订，对原有的 11 个控制进行了修改，保留了 116 个原有控制，增加了 17 个新的控制（共计 133 个控制），增加了 8 个新的控制目标（共计 39 个控制目标），5 个控制目标进行了重新的调整。新版本将大类中的组织安全变更为组织信息安全；将资产分类和控制变更为资产管理；将人员安全变更为人力资源安全；将系统的开发与维护变更为信息系统获取、开发和维护；增加从原有的类别中规整出新的大类信息安全事件管理，同时在很多子控制点中均有相应的改动。

ISO/IEC 17799:2005 新版本标准提高了外部风险的管理要求，例如针对外包、服务提供商、第三方、业务合作伙伴或客户等，并增加了服务等级协议（SLA）、审计说明；服务交付管理仍然沿用了 IT 服务管理标准 BS 15000/ISO 20000 的思想，对服务交付、第三方服务监控和审核、第三方服务服务变更管理等做了具体的说明。经过调整后的最新版本更加适应当前以及未来的信息安全态势。

3．ISO/IEC 2700X 系列标准

2005 年 10 月，BS 7799-2《信息安全管理体系规范》成功升级为国际标准，编号为 ISO/IEC 27001。ISO/IEC 27001 是信息安全管理体系（ISMS）的规范说明，它解释了如何应用 ISO/IEC 17799。其重要性在于它提供了认证执行的标准，且包括必要文档的列表。

ISO/IEC 27001 信息安全管理体系标准强调风险管理的思想。传统的信息安全管理基本上还处在一种静态的、局部的、少数人负责的、突击式、事后纠正式的管理方式，导致的结果是不能从根本上避免、降低各类风险，也不能降低信息安全故障导致的综合损失。而 ISO/IEC 27001 标准基于风险管理的思想，指导组织建立信息安全管理体系 ISMS。ISMS 是一个系统化、程序化和文件化的管理体系，基于系统、全面、科学的安全风险评估，体现预防控制为主的思想，强调遵守国家有关信息安全的法律法规及其他合同方要求，强调全过程和动态控制，本着控制费用与风险平衡的原则合理选择安全控制方式保护组织所拥有的关键信息资产，使信息风险的发生概率和结果降低到可接受的水平，确保信息的保密性、完整性和可用性，保持组织业务运作的持续性。

ISO/IEC 17799 则同时被国际标准化组织重新编号为 ISO/IEC 27002。它提供了计划和实现流程的指导，该标准也提出了一系列的控制（安全措施）。

目前，信息安全管理标准正从单一的英国国家标准 BS 7799 系列转换成更为广泛的应用的国际标准 ISO/IEC 2700X 系列。国际标准化组织（ISO）专门为 ISMS 预留出了一批标准序号。根据 ISO 的计划，ISO/IEC 2700X 系列标准的序号已经预留到 27019，其中将 27000～27009 留给 ISMS 基本标准，27010～27019 预留给 ISMS 标准族的解释性指南与文档。这一方面说明了 ISO 对 ISMS 的重视程度，也说明了 ISMS 相关标准正在各方实践的基础上不断更新和优化。2007 年由我国提交的国际标准提案《信息安全管理体系审核指南》已经成为国际标准项目，目前已进入 CD（委员会草案）阶段。下面列出了 ISO/IEC 2700X 中的一些基础标准：

- ISO/IEC 27000：原则和词汇表；
- ISO/IEC 27001：信息安全管理体系（ISMS）要求；
- ISO/IEC 27002：实用规则；
- ISO/IEC 27003：ISMS 实施指南；
- ISO/IEC 27004：ISMS 测量；
- ISO/IEC 27005：风险管理；
- ISO/IEC 27006：ISMS 审核和认证机构的要求；
- ISO/IEC 27007：ISMS 审核员指南。

4．IT 安全管理指南（ISO/IEC TR 13335）

ISO/IEC 13335《IT 安全管理指南》新版称作“信息和通信技术安全管理”，它是由 ISO/IEC 制订的技术报告，是一个信息安全管理方面的指导性标准，其目的是为有效实施 IT 安全管理提供建议和支持。其特点是强调以风险管理为核心的信息安全管理。ISO/IEC 13335 由 5 个部分标准组成，5 个组成部分分别如下：

（1）ISO/IEC 13335-1:1996《IT 安全的概念与模型》。该部分包括了对信息安全和安全管理的一些基本概念和模型的介绍。

（2）ISO/IEC 13335-2:1997《IT 安全管理与策划》。该部分建议性地描述了信息安全管理与策划的方式和要点。

（3）ISO/IEC 13335-3:1998《IT 安全管理技术》。该部分覆盖了风险管理技术、信息安全计划的开发以及实施与测试，还包括一些后续的制度审查、事件分析、信息安全教育程序等。

（4）ISO/IEC 13335-4:2000《安全管理措施的选择》。该部分主要探讨如何针对一个组

织的特定环境和安全需求来选择防护措施。

（5）ISO/IEC 13335-5：2001《网络安全管理指南》。该部分主要描述了网络安全的管理原则以及各组织如何建立框架以保护和管理信息技术体系的安全性。这一部分将有助于防止网络攻击，把使用信息系统和网络的危险性降至最低。

目前，ISO/IEC 13335-1:1996 已经被新的 ISO/IEC 13335-1:2004 所取代，ISO/IEC 13335-2:1997 也将被正在开发的 ISO/IEC 13335-2 取代。

5．信息及相关技术控制目标（COBIT）

信息及相关技术控制目标 COBIT（Control Objectives for Information and related Technology）是目前国际上通用的信息系统审计的标准，是由信息系统审计与控制协会在 1996 年发布的。它为 IT、安全、审计经理和用户提供了一套完整的参考框架。

COBIT 是以组织的业务目标为核心，为组织提供其所需的信息，同时，平衡在信息技术领域的投资与风险，把握技术发展带来的机会，以达到利益最大化，机会资本化，获取竞争优势。为了实现这些目标，COBIT 采用了层次结构的管理方法，把 IT 过程按其性质划分为 4 个域，分别为：规划与组织、获得与实施、交付与支持、监控。

目前，COBIT 已经发布了第三版，已在世界 100 多个国家的重要组织和企业中实践着，指导着这些组织最大限度地利用信息技术带来的好处，同时有效地管理与信息相关的风险。可以说，这套框架已成为国际上信息技术管理的事实标准。

6．IT 服务流程管理（ITIL）

信息技术基础设施库 ITIL（Information Technology Infrastructure Library）是由英国政府的中央计算机和通信机构（CCTA）提出的，由英国商务部（OGC）负责维护的一套 IT 服务管理标准。目前在欧洲非常盛行，在北美也日益普及，它通过描述 IT 的关键的 10 个核心流程的目标、活动、输入、输出以及各个流程之间的关系，为 IT 服务管理领域确立了一套最佳实践方法。到 90 年代中期，ITIL 已成为世界服务管理领域事实上的标准，IT 著名厂商 IBM、HP、CA 根据 ITIL 都提出了自己的服务管理模型，ITIL 在世界上得到了广泛的认可。

与 ISO/IEC 27001 相比，ITIL 关注面更为广泛（信息技术），而且更侧重于具体的实施流程，ISMS 实施者可以将 ISO 2700X 系列作为 ITIL 在信息安全方面的补充，同时引入 ITIL 流程的方法，以此加强信息安全管理的实施能力。

8.1.4 我国信息安全管理相关标准

在信息安全管理标准的制订方面，我国主要采用与国际标准靠拢的方式，充分借鉴吸收国际标准的长处。在全国信息安全标准化技术委员会内，第 7 工作组（WG7）主要负责研究和制订适用于涉密和敏感领域之外的安全保障的通用安全管理方法、安全控制措施以及安全支撑和服务等方面的标准、规范及指南。在 WG7 的努力下，目前我国已正式转化的信息安全管理国际标准有：

- GB/T 19716-2005《信息技术 信息安全管理实用规则》（修改采用国际标准 ISO/IEC 17799:2000）；
- GB/T 19715.1-2005《信息技术 IT 安全管理指南第 1 部分：IT 安全概念和模型》（等同采用 ISO/IEC TR 13335-1:1996）
- GB/T 19715.2-2005《信息技术 IT 安全管理指南第 2 部分：管理和规划 IT 安全》（等同采用 ISO/IEC TR 13335-2:1997）
- GBT 22080-2008《信息技术 安全技术 信息安全管理体系 要求》（等同采用 ISO/IEC 27001:2005）
- GBT 22081-2008《信息技术 安全技术 信息安全管理实用规则》（代替 GB/T 19716-2005，等同采用 ISO/IEC 27002:2005）

等级保护工作的开展为我国安全管理标准的制定工作提出了新的要求。在吸收原有等级

保护有关行标经验的基础上，WG7 组织完成了 2 项安全管理类行业标准的提升国标工作：GB/T 20269-2006《信息安全技术 信息系统安全管理要求》和 GB/T 20282-2006《信息安全技术 信息系统安全工程管理要求》。

8.2 信息安全管理控制措施

为了对组织所面临的信息安全风险实施有效的控制，组织要针对具体的安全威胁和薄弱点采取适当的控制措施，包括管理手段和技术方法。本节根据 ISO/IEC 27002 标准，详细介绍了信息安全方针、安全组织、资产管理、人力资源安全等 11 个方面的管理控制措施。

8.2.1 信息安全方针

1. 信息安全方针的概念

信息安全方针（Information Security Policy）本质上来说是描述组织具有哪些重要的信息资产，并说明这些信息资产如何被保护的一个计划，其目的就是对组织中成员阐明如何使用组织中的信息系统资源，如何处理敏感信息，如何采用安全技术产品，用户在使用信息时应当承担的责任，详细描述员工的安全意识与技能要求，列出被组织禁止的行为。

信息安全方针通过为组织的每一个人提供基本的规则、指南、定义，从而在组织中建立一套信息资产保护标准，防止员工的不安全行为引入风险。信息安全方针是进一步制定控制规则、安全程序的必要基础。安全方针应当目的明确、内容清楚，能广泛地被组织成员接受与遵守，而且要有足够的灵活性、适应性，能涵盖较大范围内的各种数据、活动和资源。建立了信息安全方针，就设置了组织的信息安全基础，可以使员工了解与自己相关的信息安全保护责任，强调信息系统安全对组织业务目标的实现、业务活动持续运营的重要性。

2. 信息安全政策的层次

信息安全政策可以分为两个层次，一个是信息安全方针，另一个是具体的信息安全策略。

信息安全方针是组织的管理层制订的一个高层文件，用于指导组织如何对资产，包括敏感性信息进行管理、保护的规则和指示。信息安全方针应当阐明管理层的承诺，提出组织管理信息安全的方法，并由管理层批准，采用适当的方法将方针传达给每一个员工。信息安全方针至少应该包括以下内容：

- 信息安全的定义，总体目标、范围，安全对信息共享的重要性；
- 管理层意图、支持目标和信息安全原则的阐述；
- 信息安全控制的简要说明，以及依从法律、法规要求对组织的重要性；
- 信息安全管理的一般和具体的责任定义。

具体的信息安全策略是在信息安全方针的框架内，根据风险评估的结果，为保证控制措施的有效执行而制定的明确具体的信息安全实施规则。主要包括：物理安全策略、人员审查策略、访问控制策略、网络安全策略、移动计算设施的安全策略、口令管理策略、数据备份策略、数据加密策略、灾难恢复策略、事故处理、紧急响应策略等。

8.2.2 信息安全组织

信息安全组织包括两个方面控制目标：管理组织范围内的信息安全；组织的被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全。

1. 内部组织

一个组织的管理者应通过清晰的说明、可证实的承诺、明确的信息安全职责分配及确认，来积极支持组织内的安全。管理者应识别对内外部专家的信息安全建议的需求，并在整个组织内评审和协调专家建议结果。根据组织的规模不同，这些职责可以由一个专门的管理协调小组或由一个已存在的机构（例如董事会）承担。

信息安全活动应由来自组织不同部门并具备相关角色和工作职责的代表进行协调。一般而言，信息安全协调应包括管理人员、用户、行政人员、应用设计人员、审核员和安全专员，

以及保险、法律、人力资源、IT 或风险管理等领域专家的协调和协作。

一个组织内的所有的信息安全职责应予以清晰地定义，并与信息安全方针相一致。各个资产的保护职责以及执行特定安全过程的职责都要得到清晰的识别。这些职责可在必要时加以补充，为特定地点和信息处理设施提供更详细的指南。承担安全职责的人员可以将安全任务委托给其他人员。但委托人仍是责任人，应能够确定被委托的任务得到了正确的执行。

保密协议是重要的信息安全文档。应识别并定期评审一个组织的保密性要求，并与所有人员签订保密协议。保密协议要遵循和落实所有可适用的法律法规，并定期根据具体情况变化进行修改。

一个组织在信息安全保护中需要注意与政府部门和特定利益集团的联系。要有明确的规程指明何时与哪个部门（例如执法部门、消防部门、监管部门等）联系，以及怀疑信息安全事件可能触犯法律时，应如何及时报告。对于可能来自互联网的攻击，可能还需要外部第三方（例如互联网服务提供商或电信运营商）采取有关措施。此外，也需要与特定利益集团、其他安全专家组和专业协会的适当联系，并建立信息共享协议以加强信息安全问题的协作和协调。

最后，组织的理信息安全实施方法（例如信息安全的控制目标、控制措施、方针、过程和规程）应定期进行独立评审。当发生重大变化时，也要进行独立评审。

2．外部各方

与“外部各方”有关的安全管理措施主要是为了保持组织中被外部各方访问、处理、管理或与外部进行通信的信息和信息处理设施的安全。具体包括：组织的信息和信息处理设施的安全不应由于引入外部方的产品或服务而降低；外部方对组织的信息处理设施的任何访问、对信息资产的处理和通信都应予以控制；如有与外部方一起工作的业务需要，而外部方可能要求访问组织的信息和信息处理设施，或者从外部方获得产品和服务、提供给外部方产品和服务，都应进行风险评估，以确定涉及信息安全的有关方面和控制要求。此外，在与外部方签订的协议中还应商定和定义好安全控制措施。

8.2.3　资产管理

资产管理主要包括两个方面的控制目标：对资产负责和信息分类。

1．对资产负责

对资产负责的目标是实现和保持对组织资产的适当保护。即，所有资产都是可核查的，并且有指定的责任人，并要求责任人承担对相应控制措施进行维护的职责。

资产清单可以有效地帮助组织对资产实施有效的保护，资产清单还是资产评估的重要组成部分。与信息系统相的资产主要有：信息资产，例如数据库和数据文件、系统文档、用户手册、培训资料、操作或支持程序、连续性计划、备份计划、归档信息等；软件资产，例如应用程序软件、系统软件、开发工具、实用程序等；物理资产，例如计算机设备、通信设备、可移动介质、其它技术设备等；服务，例如计算和通信服务、公共服务，包括供电、照明、供暖、空气调节等；人员，包括其资格、技能和经验；无形资产，例如组织的声誉和形象。

与信息处理设施有关的所有信息和资产都应由组织内的指定部门或人员承担责任，且信息和资产的使用规则应加以明确记录，包括资源使用的限制条件。

2．信息分类

不同的信息资产具有不同的价值属性和存在特点，存在的弱点、面临的威胁、需要进行的保护和安全控制各不相同。为此，有必要对组织中的信息资产进行科学分类，采用信息分类定义适当的安全保护等级，并根据保护等级采取必要的安全控制措施。

对信息资产进行分类时，应以其对组织的价值、法律要求、敏感性和关键性为标准，并考虑到组织的业务对于信息共享或限制的需要，以及这些需要可能对组织运营带来的影响。信息的保护等级可通过分析信息的保密性、完整性、可用性及其它要求进行评估。

除信息分类外，组织还应根据信息分类的原则，制定相应的信息标识及处理程序，以处理各类物理形式和电子形式的信息资产。对于含有敏感信息或者重要信息的资产，处理程序的输出应当带有适当的分类标识。对每类信息，应定义包括安全处理、储存、传输、删除、销毁的处理规程，以及一系列对安全相关事态的监督和记录规程。

8.2.4 人力资源安全

人力资源管理包括任用前、任用中和任用的终止和变更三个方面的控制目标。

1．任用前

任用前的控制目标是确保员工、合同方和第三方用户了解其责任并认可其角色，减少盗窃、滥用或设施误用的风险。

安全角色和职责应于任用前按照组织的信息安全方针进行定义并形成文档。特别重要的是，还应清晰定义未在组织任用过程（例如通过第三方组织任用）中任用的个人的安全角色和职责。

要按照相关法律法规、道德规范和对应的业务要求，以及被访问信息的类别和可能的风险，实施对所有候选任用者和第三方人员的背景验证核查程序。

作为任用合同的一部分，雇员、合同方人员和第三方人员应同意并签署其任用合同的条款和条件，这些条款和条件中应声明他们和组织的信息安全职责。

2．任用中

在任用过程中，应确保所有的员工、合同方和第三方人员了解信息安全威胁和相关事宜，以及他们的责任和义务，并在日常工作中支持组织的信息安全方针，减少人为错误的风险。

管理者应要求雇员、合同方人员和第三方人员按照组织已建立的方针策略和规程对安全尽心尽力，并组织的所有雇员，包括合同方人员和第三方人员，接受与其工作职能相关的。

对于安全违规的雇员，应有正式的纪律处理过程。这一纪律处理过程应确保正确和公平地对待被怀疑安全违规的雇员，且应该是分级的，即考虑例如违规的性质、重要性及对于业务的影响等因素，以及相关法律、业务合同等因素。纪律处理过程很重要，它可用于对雇员、合同方人员和第三方人员的威慑，防止他们违反组织的安全方针、规程及其他安全违规。

3．任用的终止和变更

任用的终止和变更的目标是确保雇员、合同方和第三方用户离开组织或任用变更时以一种有序的方式进行。应对雇员、合同方和第三方用户从组织中退出的过程进行管理，并确保他们归还所有设备及删除他们的所有访问权。

应清晰规定和分配进行任用终止或变更的责任。在雇员、合同方或第三方用户的合同中，应规定哪些职责和义务在任用终止后仍然有效。职责和工作的变更管理与此类似，也应严格管理。

当任用、合同或协议终止时，雇员、合同方和第三方用户应归还所使用的组织资产。如雇员、合同方或第三方用户已购买了组织的设备或使用了他们自己的设备时，应确保设备中所有相关的信息已转移给了组织，并且已从设备中安全地删除。

另外，当任用、合同或协议终止时，应撤销所有雇员、合同方和第三方用户对信息和信息处理设施的访问权限，或根据变化调整。如工作终止，个人对与信息系统和服务有关的资产的访问权力应得到重新考虑，需删除或改变的访问权包括物理和逻辑访问、密钥、ID卡、信息处理设备、签名等。如已离职雇员、合同方或第三方用户知道仍保持活动状态的账户的密码，则应在工作、合同或协议终止或变化后及时改变密码。

8.2.5 物理和环境安全

物理和环境安全包括安全区域和设备安全两个方面的控制目标。

1．安全区域

安全区域的目标是防止组织的场所和信息受到未经授权的物理访问、损害和干扰。为了

达到这一目标，应当把关键和敏感的信息处理设备放在安全区域内，并受到确定的安全周边的保护，保护适当的安全屏障和入口控制。这些设施应从实体上加以保护，避免未授权访问、损坏和干扰，且所提供的保护应与所识别出的风险相匹配。具体的控制措施涉及到：

- 物理安全周边
- 物理入口控制
- 办公室、房间和设施的安全保护
- 外部和环境威胁的安全防护
- 在安全区域工作
- 公共访问、交接区安全

2．设备安全

设备安全的目标是防止资产的流失，保护设备免受损坏或破坏，从而达到业务的正常运行，使其免于安全风险和环境灾难。

关于设备安全，一般应考虑以下方面：

一是妥善安置和保护设备，以降低环境威胁和灾难风险，减少未经授权的访问。

二是使设备免于因支持性设施的失效而引起的电源故障和其它中断。

三是保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听或损坏。

四是对设备进行正确维护，以确保其持续的可用性和完整性。

五是对组织场所外的设备采取安全措施，要考虑工作在组织场所以外的不同风险。

六是设备的安全处置及再利用问题，避免不适当的设备处置及再利用会危及信息安全。

七是资产的移动问题。在未经授权的情况下，不能把设备、信息或者软件转移到工作场所以外，同时应当进行现场检查以防止未经授权的信息资产被转移。

8.2.6 通信和操作管理

通信和操作管理的控制目标包括操作规程和职责、第三方服务交付管理、系统规划与验收、防范恶意和移动代码、备份、网络安全管理、介质处理、信息交换、电子商务服务、监视等方面。

1．操作规程和职责

为了确保信息系统中的信息处理设备正确无误地安全运行，明确信息处理设备的管理与操作责任、程序（包括建立操作指南和事故处理程序），是保证系统安全运行的最基本的也是最主要的管理措施。为此，应实现操作规程文档化，加强变更管理，并实施责任分割策略。特别是，作为一项通用的管理措施，应当考虑把某些责任、责任区域的管理或执行加以分离，减少对系统或者服务未经授权的访问或者改动的机会。

此外，还应实现开发、测试和运行过程的分离，避免在软件开发和测试的过程中因某些文件或系统环境的改动而对运行环境造成某种程度的影响。

2．第三方服务交付管理

为了使第三方服务交付协议符合信息安全的要求，使第三方服务的交付达到适当水准，组织应对协议进行核查，监视协议的执行，并管理协议的变更，以确保交付的服务能够满足与第三方商定的所有要求。

3．系统规划与验收

在信息系统建立之前，为保证日后系统的正常运行，将系统产生故障的风险降低到最小，应对所建立的系统进行风险分析和风险评估，进而对系统进行策划和验收。有关管理措施包括以下方面：

- 容量管理。为了确保系统有足够的处理能力和存储空间可供利用，应当监测当前系统容量的需要并预测对未来的容量需求，这些预测中应当考虑到新的业务需求和系统需求，以及组织当前的和预测的信息处理趋势。

- 系统验收。当系统建立或升级之后，应根据验收标准进行验收，并在验收之前根据相关的技术要求对系统进行测试。

4．防范恶意和移动代码

恶意代码是信息系统常见的威胁，后果有时极为严重，因此必须采取有效措施防范和检测恶意和未授权移动代码的引入，保护软件和信息的完整性。

恶意代码的防范应基于恶意代码校验和、修复软件、安全意识培训、适当的系统访问和变更管理控制措施等手段，可考虑的规定有：建立禁止使用未授权软件的正式策略，建立使用外部网络或其它介质上的文件和软件的策略，建立对支持关键业务过程的系统中的软件和数据内容进行定期评审的策略，建立安装和定期更新恶意代码检测和修复软件的策略，制定适当的从恶意代码攻击中恢复的业务连续性计划，建立定期收集恶意代码相关信息的规程。

为防止移动代码执行未授权的活动，可考虑下列措施：在逻辑上隔离的环境中执行移动代码，阻断移动代码的所有使用，阻断移动代码的接收，将恶意代码限制在一个特定系统中可用，控制移动代码访问的可用资源，使用密码技术来对移动代码进行鉴别。

5．备份

为了保持信息及信息处理设施的完整性和可用性，应采取有效措施定期对基本业务信息和软件进行备份，这是保证信息系统正常运行必不可少的重要环节。因此，需要有足够的信息备份设备作保证，所有重要的业务信息和软件都能在一次事故或存储介质故障之后迅速得到恢复。

信息备份主要考虑如下因素：应定义备份信息的必要级别；要有对备份拷贝的准确完整的记录和文档化的恢复程序；备份的程度和频率符合组织的业务需求；备份要存储在一个远程地点，以避免主场地的灾难事件；对备份信息给予适当程度的物理和环境保护；定期测试备份介质和备份程序；重要的业务信息，应明确规定保存时间，必要时采用加密手段进行保护等。

6．网络安全管理

为了确保网络中的信息和支持性基础设施得到保护，应对网络进行充分的管理和控制，包括以下方面：

- 网络控制。确保网络上的信息安全、防止未授权访问网络所连接的服务。特别要考虑以下管理措施：网络的操作职责要与计算机操作分开；应建立远程设备（包括用户区域内的设备）管理的职责和程序；要建立专门的控制，以保护在公用网络上传输数据的保密性和完整性，保护已连接的系统，维护网络服务和计算机的可用性；使用适当的日志记录和监控措施记录安全相关的活动等。
- 网络服务安全。组织应能识别所有网络服务的安全特性、服务等级和管理要求。为此，组织应确定网络服务提供商具有以安全方式管理商定服务的能力，并定期监控，必要时，还应商定审计的权力。此外，组织还应能识别特殊服务的安全配置，例如其安全特性、服务级别和管理要求。组织还应确保网络服务提供商实施了这些相应的措施。

7．介质处理

存储介质上存储着大量的十分有用的信息数据、程序等，是确保信息系统正常运行不可缺少的部分。因此，对于存储介质应得到妥善的管理和物理上的保护，使它们免遭破坏、偷盗和未经授权的访问。为此，应加强移动介质的管理，妥善销毁不使用的介质，加强信息处理程序的规范化。此外，还应重视系统文档安全，防止系统文档被未经授权访问。

8．信息交换

目前，各个不同组织间的数据交换正越来越频繁，由于被交换的信息可能被丢失、修改或盗用，因此这种信息交换必须严格受到控制，并符合所有相关的法律法规。首先，应当定

义清晰的信息交换的策略和程序，签订信息交换协议，加强转运时介质的安全。特别是，应重视电子消息安全以及业务信息系统相关信息的安全。

9．电子商务服务

电子商务服务是一种重要的信息化应用，应确保电子商务服务的安全及其安全使用，包括在线交易和控制的要求，以及通过公共可用系统以电子方式公布的信息的完整性和可用性。

10．监视

监视的目的是检测未经授权的信息处理活动。主要的措施包括：对用户活动、异常和信息安全事态进行审计；建立信息处理设施的监视使用规程，并经常对监视的结果进行审查；对日志记录设施和日志信息加以保护，防止篡改和未授权的访问；在日志中记录系统管理员和系统操作员的活动；对所有故障进行记录和分析，并采取适当的措施；确保所有相关信息处理设施的时钟使用已设的精确时间源进行同步，使日志记录中的时间信息保持一致。

8.2.7 访问控制

访问控制的目标包括访问控制的业务要求、用户访问管理、用户职责、网络访问控制、操作系统访问控制、应用和信息访问控制、移动计算和远程工作等方面。

1．访问控制的业务要求

为保护系统及其数据不被未经授权的非法访问，应首先制定完善的安全控制策略，为信息系统构建一套完整的访问安全体系，通过策略的实施最大限度地使系统及其数据因非正常的因素遭到破坏的可能性降低到最低。

访问控制策略主要考虑以下内容：各个业务应用的安全需求；与业务应用相关的所有信息的标识和信息面临的风险；信息传播和授权的策略；不同系统和网络的访问控制策略和信息分类策略之间的一致性；组织内常见工作角色的标准用户访问轮廓；访问控制角色的分离，例如访问请求、访问授权、访问管理等；在分布式和网络化环境中访问权限的管理等。

2．用户访问管理

为防止对计算机信息系统的未经授权的访问，应建立一套控制对信息系统和服务访问权限分配的程序。这些程序覆盖用户访问全过程的每一个阶段，从注册到销毁。在特殊情况下，应当特别注意对特权访问权限分配的控制。在这项管理措施中，需要注意以下环节的工作：

- 用户注册
- 特权管理
- 用户口令管理
- 用户权限的审查

3．用户责任

为避免未授权用户的访问，已授权用户的合作是有效安全的基础，要使用户了解其对维护有效的访问控制的职责，特别是关于口令的使用和用户设备的安全的职责。此外，实施桌面清空和屏幕清空策略也极为重要，用以降低未授权访问或破坏纸、介质和信息处理设施的风险。

4．网络访问控制

为保护网络服务，包括增值服务，应控制对内部和外部网络服务的访问，这是确保网络安全的关键。

实施网络访问控制的关键点有：

- 明确网络服务的使用策略
- 对外部连接用户进行认证
- 利用网络设备标识实施访问控制
- 对远程诊断和配置端口实施特别保护

- 必要时考虑网络隔离
- 对网络连接进行控制
- 对网络路由选择进行控制

5．操作系统访问控制

为了防止对操作系统的未授权访问，操作系统安全设施应该用来限制授权用户访问操作系统，包括：按照已定义的访问控制策略和认证手段鉴别授权用户，并记录成功和失败的系统鉴别尝试，记录专用系统特权的使用，恰当地限制用户的连接次数，发现违背系统安全策略时及时发布警报等。

6．应用和信息访问控制

为防止保存在信息系统中的应用系统信息被未经授权的访问，应使用安全设施限制对应用系统的访问，安全设施应该将访问限制在应用系统之内。应用系统应该做到：按照定义的访问控制策略，控制用户访问信息和应用系统功能；防止能够越过系统控制或应用控制的任何实用程序、操作系统软件和恶意软件进行未授权访问；不会损坏共享信息资源的其他系统的安全。

7．移动计算和远程工作

移动计算和远程工作使得员工可以通过使用通信技术在组织之外的固定或非固定场所进行远程工作，这些工作场所的使用环境一般情况下是不受保护的，如果不采取有效的管理措施，会对组织的信息系统造成严重的安全隐患。

为加强移动计算和远程工作时的安全保护，应考虑以下几种情况：

- 移动计算及其通信保护。移动计算策略包括对物理保护、访问控制、密码技术、备份和病毒防护的要求，还包括关于移动设施与网络连接的规则和建议，以及关于在公共场合使用这些设施的指南。
- 远程工作保护。应考虑下列内容：远程工作场地的物理安全；通信安全要求；住处的其他人员（例如家人和朋友）未授权访问信息或资源的威胁；家庭网络的使用和无线网络服务配置的要求或限制；针对私有设备开发的知识产权规定；法律禁止的对私有设备的访问；使组织对雇员、承包方人员或第三方人员等私人拥有的工作站上的客户端软件负有责任的软件许可协议；防病毒保护和防火墙要求。

8.2.8 信息系统获取、开发和维护

信息系统的获取、开发和维护的控制目标涉及信息系统的安全要求、应用中的正确处理、密码控制、系统文件的安全、开发和支持过程中的安全、技术脆弱性管理等方面。

1．信息系统的安全要求

信息系统的安全要求是指采取措施保证在开发的系统中建立有效的安全机制，包括操作系统、信息基础设施、业务应用软件、用户定制的应用软件等。

在建立新的信息系统或对现有的信息系统进行业务更新时，要在需求说明中规定安全控制的要求。安全控制和要求应能反映所涉及的信息资产的价值、可能存在的安全故障或缺乏系统安全可能导致的潜在业务损失。

信息系统的安全需求与安全实施过程应在信息安全工程的早期阶段集成。此外，对产品的采购也应提出安全要求，必要时进行安全测试。

2．应用中的正确处理

为确保应用系统安全，应采取安全措施，防止应用系统信息的错误、丢失、未授权的修改或误用。需要关注的处理环节包括：

- 输入数据确认
- 内部处理控制
- 消息完整性

- 输出数据确认

3．密码控制

密码控制的要求是通过密码技术保护信息的保密性、真实性和完整性。

一个密码解决方案是否合适，需要根据广泛的风险评估和选择控制来做出决定。制定密码策略时，应该考虑的内容包含：跨越组织使用密码控制的管理方法；基于风险评估确认的保护等级，包括所需要的加密算法的类型、强度和质量；密钥管理方法，包括密码密钥的保护，密钥遗失、泄密和毁坏后加密数据的恢复等。

当实施整个组织的密码策略时，必须考虑相关的法律、法规，确保符合国家的密码管理法律法规。

除密码使用策略外，还必须进行有效的密钥管理。所有的密码密钥都要防止被修改、遗失和毁坏。另外，秘密和私有密钥需要防止非授权的泄露。用来生成、贮存和归档密钥的设备需要进行物理保护。

4．系统文件的安全

为确保系统文件的安全，要求采取措施，保护运行软件、系统测试数据以及源程序代码的安全。

对操作系统软件，应建立起操作系统软件的安装、升级、配置等控制措施，使运行系统被损害的风险降至最低。在系统测试时，应尽量避免使用应用系统数据库中的实际的业务数据。对程序源代码，应施加特别严格的访问控制程序。

5．开发和支持过程中的安全

业务应用软件系统在开发和维护的过程中往往会遇到应用系统的业务发生了某些变化，或系统版本需要升级，此时必须对应用系统中相应部分的软件作改动，而且这种改动需经复查，以证明不会损害系统和运行环境的安全。这方面应该关注的内容有：

- 变更控制规程
- 操作系统变更后的技术检查
- 软件包的变更限制
- 掩盖和调整系统和通信的行为以防止信息泄露
- 软件包的委外开发

6．技术脆弱性管理

信息系统的脆弱性是导致安全事件的重要原因，必须建立严格的脆弱性管理流程，并以一种有效的、系统的、可重复的，并可测量的方式实施，以降低攻击者利用脆弱性危害系统的风险。所需考虑的脆弱性包括操作系统的脆弱性，也包括任何其它应用程序中的脆弱性。

应确保及时获取有关信息系统最新技术脆弱性的信息，评价组织对这些脆弱性的暴露程度，并积极采取适当的措施。

在对系统安装补丁、修复技术脆弱性时，必须对补丁进行充分的测试。如由于成本或其它资源缺乏，则可以考虑推迟补丁安装，以便基于其他用户报告的经验来评价相关的风险。但在此之间，应采取临时性措施进行风险防范。

8.2.9 信息安全事件管理

信息安全事件管理包括两个方面的控制目标：报告信息安全事件和弱点、信息安全事故管理和改进。

1．报告安全事件和弱点

报告安全事故和缺陷的目标是确保与信息系统有关的安全事件和缺陷能够及时得到汇报并采取适当的纠正措施。应准备好正常的事件报告和分类程序，及时报告可能对组织的资产安全造成影响的不同种类的事件和弱点。

2．信息安全事故管理和改进

信息安全事故管理和改进的目标是确保使用持续有效的方法管理信息安全事故。一旦信息安全事件和弱点报告上来，应该立即明确责任，按照规程进行有效处理。应该实施连续性的改进过程，对信息安全事故进行响应、监视、评估和总体管理。如果信息安全事件涉及到民事或刑事的诉讼，则需要搜集证据，以满足法律的要求。

8.2.10 业务连续性管理

业务连续性管理的控制目标是防止业务活动中断，保证重要业务流程不受重大故障和灾难的影响。为了实现这一控制目标，应该执行业务连续性管理程序，通过预防性和恢复性措施相结合，将灾难和安全事故造成的影响降低到可以接受的水平；应该对灾难事故、安全故障和服务损失所造成的结果进行分析；应当制订并实施紧急事件处理计划，确保能够在要求的时间内恢复业务流程，并应当保持这种计划，使之成为其它管理程序的一部分；业务连续性管理还应当包括相关的管理测试来识别并减少风险、限制毁灭性事件的后果、确保重要操作及时恢复。

为了在整个组织内保持业务的连续性，应当有适当的管理程序，将以下要素集成在一起：

- 根据风险的可能性及其影响，推断组织所面临的风险；
- 确定关键业务流程中涉及的所有资产；
- 推断由信息安全事故引起的业务中断对业务可能产生的影响，并且建立信息处理设施的业务目标；
- 考虑购买相应的保险，该保险可以形成业务连续性过程的一部分，也作为运行风险管理的一部分；
- 确定和考虑实施进一步的风险预防和减缓控制措施；
- 确定足够的财务的、组织的、技术的和环境的资源去满足特定的信息安全需求；
- 确保人员的安全，保护信息处理设备和组织资产；
- 按照已商定的业务连续性策略，制定应对信息安全要求的业务连续性计划，并将其形成文档；
- 定期测试和更新已有的计划和过程；
- 确保把业务连续性的管理包含在组织的过程和结构中。业务连续性管理过程的职责应分配给组织范围内的适当级别的管理层。

要确保业务的连续性，应该首先确定可能引起业务流程中断的事件，例如设备故障、人为错误、盗窃、水灾、火灾、恐怖事件等。然后，再进行风险评估，确定中断可能造成的影响，例如破坏程度和恢复时间。完成风险评估后，应根据风险评估结果，制定业务连续性战略，确定业务连续性总体规划。

8.2.11 符合性

符合性包括三个方面的控制目标：与法律法规要求的符合性，与安全策略、标准以及技术要求的符合性，以及信息系统审计考虑。

法律法规要求符合性的目标是避免违反法律、法规、规章、合同要求以及其他相关的安全要求。信息系统的设计、运行、使用和管理都要受到法律法规要求的限制，同样也会受到合同安全要求的限制，因而对法律法规要求的符合性应该首先受到关注。此外，对知识产权的保护、组织中重要记录的保护、对个人数据的保护、对滥用信息处理设施的规定、密码的控制措施等都是法律法规符合性提出的要求。

符合性的第二方面是对安全策略、标准的符合性以及技术符合性。管理层应对自己职责范围内的信息处理是否符合安全策略、标准和其它安全需求进行定期检查，出现问题时及时纠正。技术符合性检查则是确定信息系统与安全实施标准的符合程度，甚至可以使用渗透行攻击手段。

目前，国际上普遍兴起了信息系统审计项目。信息系统审计考虑的涵义是，使信息系统审计的有效性最大化，干扰最小化。这里包含两点：涉及对运行系统核查的审计要求和活动，应谨慎地加以规划并取得批准，以便使造成业务过程中断的风险最小化；对于信息系统审计工具的访问应加以保护，以防止任何可能的滥用或损害。

8.3 信息安全管理体系

信息安全管理体系 ISMS（Information Security Management System）是组织基于业务风险方法，建立、实施、运行、监视、评审、保持和改进信息安全的体系，是一个组织整个管理体系的一部分，它包括组织结构、方针策略、规划活动、职责、实践、规程、过程和资源。

当前，以 ISO/IEC2700X 为基础，建立信息安全管理体系（ISMS），已经成为很多组织开展信息系统安全建设的基本方法，围绕 ISMS 的标准、实施方案、培训、咨询服务、认证活动层出不穷，极大地推动了信息安全管理标准的应用。很多组织通过建设 ISMS，或参照 ISMS 的要求优化信息安全管理措施，明显提高了其信息安全管理水平和防护能力。

8.3.1 PDCA 模型

1．PDCA 循环概述

PDCA 循环是 ISMS 实施方法的核心理念，该概念最早是由美国质量管理专家戴明提出来的，所以又称为“戴明环”。PDCA 4 个英文字母及其在 PDCA 循环中所代表的含义如下：

- P（Plan）：计划，确定方针和目标，确定活动计划；
- D（Do）：实施，实际去做，实现计划中的内容；
- C（Check）：检查，总结执行计划的结果，注意效果，找出问题；
- A（Action）：行动，对总结检查的结果进行处理，成功的经验加以肯定并适当推广、标准化；失败的教训加以总结，以免重现；未解决的问题放到下一个 PDCA 循环。

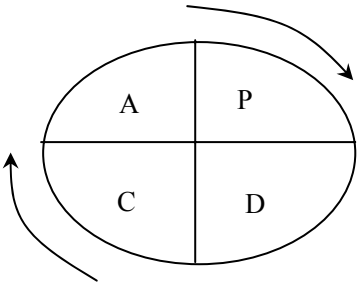


图 8-1　PDCA 循环的基本模型

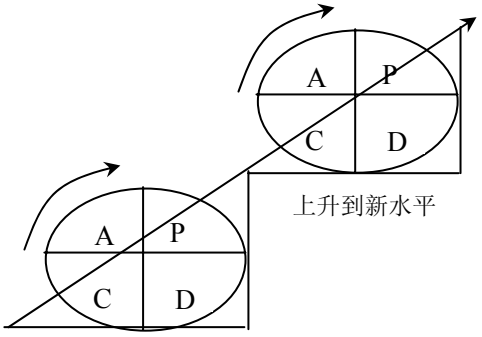


图 8-2　PDCA 循环的步骤和方法

PDCA 循环实际上是有效进行任何一项工作的合乎逻辑的工作程序，在质量管理中得到了广泛的应用，并取得了很好的效果，因而 PDCA 循环被称为是质量管理的基本方法。之所以称之为 PDCA 循环，是因为这 4 个过程不是运行一次就结束，而是周而复始地进行。一个循环结束了，可能还有其他的问题尚未解决，或者又出现的新的问题，再进入下一次循环，如此反复，其基本模型见图 8-1 所示，PDCA 循环的步骤和方法则入图 8-2 所示。

2．PDCA 循环的特点

PDCA 循环具有以下三个特点：

（1）大环带小环。如果把整个企业的工作作为一个大的 PDCA 循环，那么各个部门、小组还有各自小的 PDCA 循环，就像一个行星系一样，大环带动小环，一级带一级，有机地构成一个运转的体系。

（2）阶梯式上升。PDCA 循环是螺旋式上升和发展的，每循环一次，就解决一部分问题，取得一部分成果，工作就前进一步。到了下一次循环，又有了新的目标和内容，更上一

层楼。见图 8-2 表示了 PDCA 循环的步骤和方法。

（3）科学管理方法的综合应用。PDCA 循环应用以 QC（质量控制）七种工具为主的统计处理方法以及工业工程（IE）中工作研究的方法作为进行工作和发现、解决问题的工具。

3．信息安全管理的 PDCA 循环

信息安全管理的 PDCA 模式从安全需求和期望出发，将安全管理的计划、实施、检查和改进 4 个环节链接成一个环状的循环过程，在每个环节中适应风险的变化而变化，并从一个环节适度地过渡到下一个环节，体现了安全管理的动态性；同时，它循环往复，环节之间密切衔接，体现了安全管理的持续性，见图 8-3 所示。

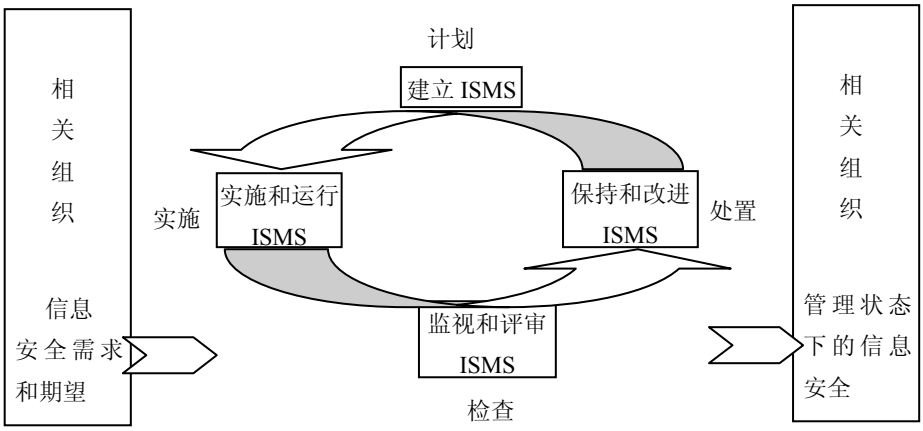


图 8-3　信息安全管理的 PDCA 循环

图 8-3 中，“P”、“D”、“C”、“A”分别表示的意思是：

（1）计划（建立 ISMS）：建立与管理风险和改进信息安全有关的 ISMS 方针、目标、过程和规程，以提供与组织总方针和总目标相一致的结果。

（2）实施（实施和运行 ISMS）：实施和运行 ISMS 方针、控制措施、过程和规程。

（3）检查（监视和评审 ISMS）：对照 ISMS 方针、目标和实践经验，评估并在适当时测量过程的执行情况，并将结果报告管理者以供评审。

（4）处置（保持和改进 ISMS）：基于 ISMS 内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进 ISMS。

8.3.2　建立 ISMS

建立信息安全管理体系首先要建立一个合理的信息安全管理框架，要从整体和全局的角度，从信息系统的所有层面进行整体安全建设，并从信息系统本身出发，通过建立资产清单，进行风险分析、需求分析和选择安全控制等步骤，建立安全体系并提出安全解决方案。

本阶段的主要工作有：定义信息安全政策；确定信息安全管理体系的范围；定义风险评估的系统性方法；识别风险；评估风险；识别并评价风险处理的方法；为风险的处理选择控制目标与控制方式；获得管理层的授权批准等。

进行安全管理框架的搭建需按适当的程序进行。组织首先应根据自身的业务性质、组织特征、资产状况和技术条件定义 ISMS 的总体方案和范围，然后在风险分析的基础上进行安全评估，同时确定信息安全风险管理制度，选择控制目标，准备适用性声明。具体过程见图 8-4 所示。

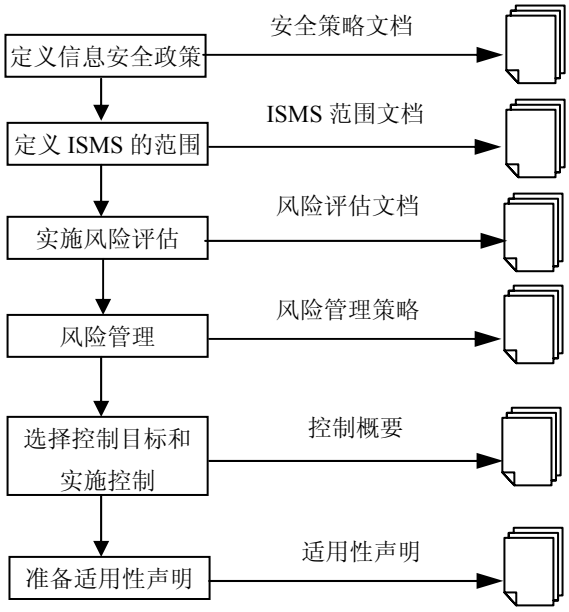


图 8-4　建立信息安全管理系统的步骤

1．确定信息安全政策

信息安全政策可以分为两个层次，一个是信息安全方针，另一个是具体的信息安全策略。

信息安全方针必须要在 ISMS 实施的前期制定出来，表明最高管理层的承诺，指导 ISMS 的所有实施工作；信息安全策略的制订要在风险评估工作完成后，对组织的安全现状有了明确的了解的基础上有针对性的编写，用于指导风险的管理与安全控制措施的选择。需要根据组织内各个部门的实际情况，分别制订不同的信息安全策略。例如，规模较小的组织单位可能只有一个信息安全策略，并适用于组织内所有部门、员工；而规模大的集团组织则需要制订一个信息安全策略文件，分别适用于不同的子公司或各分支机构。信息安全策略应该简单明了、通俗易懂，并形成书面文件，发给组织内的所有成员。同时要对所有相关员工进行信息安全策略的培训，对信息安全负有特殊责任的人员要进行特殊的培训，以使信息安全方针真正植根于组织内所有员工的脑海并落实到实际工作中。

2．确定 ISMS 的范围

ISMS 的范围就是需要重点进行信息安全管理的领域，组织需要根据自己的实际情况，在组织的所有信息系统、部分信息系统以及特定信息系统内构架 ISMS。在本阶段，应将组织划分成不同的信息安全控制领域，以易于组织对有不同需求的领域进行适当的信息安全管理。在定义 ISMS 范围时，应重点考虑组织的如下实际情况：

（1）组织现有部门。组织内现有部门和人员均应根据组织的信息安全方针和策略，负起各自的信息安全职责。

（2）办公场所：有多个办公场所的组织单位，应该考虑不同办公场所给信息安全带来的不同安全需求和威胁。

（3）资产状况：在不同地点从事商务活动时，应把在不同地点涉及到的信息资产纳入到 ISMS 管理范围内。

（4）所采用的技术：使用不同计算机和通信技术，将会对信息安全分为的划分产生很大的影响。

3．实施风险评估

风险评估首先要对 ISMS 范围内的信息资产进行鉴定和估价，然后对信息资产面对的各种威胁和脆弱性进行评估，同时对已存在的或规划的安全控制措施进行鉴定。信息安全风险

评估的复杂程度将取决于业务信息和系统的性质、使用信息的组织业务目标、所采用的系统环境、以及受保护资产的敏感程度。所采用的评估措施应该与组织对信息资产风险的保护需求相一致，组织需要将直接后果和潜在的后果一并考虑。

4．管理风险

通过风险评估与现状调查的结果，组织要决定在安全方针的范围内，如何对信息资产实施保护以及保护到何种程度。这个阶段主要涉及以下几个方面的工作：

1）确定安全需求

组织的安全需求描述了组织信息安全的目标与需求。一般来说，企业安全需求可以从以下三个方面来考虑：

- 来自风险的安全需求
- 来自法律、法规、合同的需求
- 来自业务的需求

2）选择风险管理方法

通过风险评估的结果、组织的业务和法律法规对信息安全的需求分析，组织就可以得到总的安全需求。为满足总的安全需求，可以通过以下四种方法进行风险管理：

- 避免风险
- 降低风险
- 转移风险
- 接受风险

3）建立风险管理策略

风险管理策略是在信息安全方针的基础上，根据风险评估的结果，为降低信息安全风险，保证控制措施的有效执行而制定的明确具体的信息安全实施规则。这种策略是原则性的、通用性较强，并与信息安全方针一起汇编成《信息安全手册》，在组织最高管理层的批准下，在组织中强制执行。

5．选择控制目标和控制对象

对控制目标与控制需求的选择应当由安全需求来驱动，控制的选择应当是基于最好地满足安全需求，并要考虑安全需求得不到满足时的后果。一般来说，控制的选择可以按以下过程来进行：

- 考虑对基于业务与法律法规的安全需求
- 考虑对基于风险分析的安全需求
- 考虑组织必须关注的各种安全问题

6．适用性声明

在风险评估之后，组织应选用标准中符合组织自身需要的控制措施与控制目标。所选择的控制目标和控制措施以及被选择的原因应在适用性声明（SOA，Statement of Application）中进行说明。SOA 应包括的内容有：选择的控制目标和控制措施以及选择的原因、最新实施的控制目标和控制措施、标准中控制目标和控制措施的删减以及删减的合理性。

SOA 是适合组织需要的控制目标和控制的评论。需要提交给管理者、职员、具有访问权限的第三方相关认证机构。

SOA 的准备，一方面是为了向组织内的员工声明对信息安全面对的风险的态度，在更大的程度上则是为了向外界表明组织的态度和作为，以表明组织已经全面、系统地审视了组织的信息安全系统，并将所有需要控制的风险控制在能够被接受的范围内。

8.3.3 实施和运行 ISMS

信息安全管理体系文件编制完成之后，组织便可按照文件的要求进行审核与批准并发布实施。本阶段的任务是以适当的优先权进行管理运作，执行所选择的控制，以管理计划阶段

所识别的信息安全风险。

本阶段的主要工作有：建立一个有效的管理体系（机制）；依据规定的方式方法监控计划阶段所提的活动；确保计划阶段未预料的影响和破坏被快速识别并得到适当管理；分配适当的资源（人员、时间和资金）运行信息安全管理体系以及所有的安全控制；安排针对信息安全意识的培训，并检查意识培训的效果；实施并保持已计划好的检测和响应机制。下面介绍其中的几个关键问题：

1．保证资源、提供培训、提高安全意识

应该为信息安全管理体系的运行和所有安全控制措施的实施提供充足的资源，提供实施所有控制措施的相关文件，并对信息安全管理体系文件进行维护。另外，还应该进行信息安全教育活动，以提高员工安全意识，在组织中产生良好的风险管理和安全的文化；并对员工进行有关信息安全技能与技术的培训，使员工掌握信息安全的实现手段。

2．风险管理

对于经过评估可以接受的风险，不需要进一步采取措施。对于经过评估不可接受的风险，可以采取降低风险或转移风险的方法进行风险处理。如果决定转移风险，应该采取签订合同，参加保险的方式，或采取灵活的组织结构（如寻找合资伙伴）等进一步行动。无论哪一种情况，都必须保证风险转移到的组织能理解风险的性质，并且能够有效地管理这些风险。如果组织决定降低风险，就要在 ISMS 范围内实施已选择的降低风险的控制措施。这些实施措施应与计划活动中准备的风险控制计划相一致。

成功实施计划要求有效的管理体系，管理体系定义了选择的控制目标与控制措施，落实责任和控制的过程，以及监控这些控制的过程。当一个组织决定接受高于可接受水平的风险时，应获得管理层的批准。在不可接受风险被降低或转移之后，还会有残余风险，控制措施应保证残余风险所产生的影响或破坏能及时被识别并适当管理。

总之，本阶段的工作内容包括：建立一个有效的管理机制；依据规定的方式方法监控计划阶段所提的活动；确保计划阶段未预料的影响和破坏被快速识别并得到适当管理；分配适当的资源（人员、时间和资金）运行信息安全管理体系以及所有的安全控制；安排针对信息安全意识的培训，并检查意识培训的效果；实施并保持已计划好的探测和响应机制。

8.3.4 监视和评审 ISMS

监视和评审的主要任务是进行有关方针、程序、标准与法律法规的符合性检查，如果发现一个控制措施不合理、不充分，就要采取纠正措施，以防止信息系统处于不可接受的风险状态。

本阶段的主要工作有：执行监视程序和其他控制措施以快速检测处理结果中的错误；评审信息安全管理体系的有效性，收集安全审核、事故、有效性测量的结果以及所有相关方的建议和反馈；评审剩余风险和可接受风险的等级；审核规定的安全程序是否适当、是否符合标准以及是否按照预期的目的进行工作；正式评审；记录并报告有可能影响信息安全体系有效性或执行的措施和事件等。

检查活动应该对采用的控制措施与实施过程进行描述，内容包括：对风险的不间断评审，在技术、威胁或功能不断变化的情况下，对管理风险的方法和过程的调整。在确定当前的安全状态令人满意的同时，应注意技术的变化、业务的需求与新威胁和脆弱点的出现，尽量预测信息安全管理体系将来的变化，并采取有效措施确保其在将来持续有效地运转。常用的检查措施主要有以下几种：

1．日常检查

日常检查应作为正式的业务过程经常进行，并设计用来侦测处理结果的错误。日常检查可能包括：调整银行账户、资产清点、解决客户抱怨等。这类的检查需要设计在 ISMS 体系中，以完备的检查措施来限制由错误造成的损害。

在 ISMS 中此类的检查可以扩展到：检查对系统软件、管理软件参数与数据的非授权修改以及确定数据在网络传输中的准确性和完整性。

2．自治程序

自治程序是一种为了保证任何错误或失败在发生时能够被及时发现而建立的控制措施。例如，网络设备发生故障或错误，监控程序或监控设备可以自动报警。警报能够提醒负责的员工解决存在的问题，帮助他们完整查清事故原因并修复存在的问题。如果在一段时间内问题不能被纠正，另外的报警会通知更高层的管理者。

3．学习其他组织好的经验

可以学习其他组织在处理此类问题时是否有更好的办法。这种学习适用于技术和管理活动。组织可以利用很多资源来识别技术管理中的脆弱性。例如，管理技巧的信息经常会在很多论坛上交流和讨论，包括：会议、行业协会和使用者小组，有很多文件发布在技术和管理杂志上。

4．信息安全管理体系审核

信息安全管理体系的审核是组织为验证所有的安全方针、策略、程序的正确实施和检查信息系统符合安全实施标准的情况所进行的系统的、独立的检查和评价，是信息安全体系的一种自我保证手段。审核结果是一系列不符合行为或者观察结果，以及相应的校正行动的报告。

信息安全体协审核包括管理和技术两方面的审核，管理性审核主要是定期检查有关安全方针、策略与程序是否被正确有效地实施；技术性审核是指定期检查组织的信息系统符合安全实施标准的情况，技术性的审核需要信息安全技术人员的支持，必要时会使用系统审核工具。

组织应建立并保持审核方案和程序，定期开展信息安全管理体系的审核，以保证它的文件化过程，信息安全活动以及实施记录能够满足标准要求和声明的范围，检查信息安全实施过程符合组织的方针、目标和策划要求，并向管理者提供审核结果，为管理者的信息安全决策提供支持。

ISMS 审核的主要目的如下：

- 检查标准的实施程度及与标准的符合性情况；
- 检查满足组织安全策略与安全目标的有效性和适用性；
- 识别安全漏洞与弱点；
- 提供给管理者 IT 安全控制目标实现状况，使管理者了解 IT 安全问题；
- 指出存在的重大的控制弱点，证实存在的风险；
- 建议管理者采取正确的校正行动，为管理者的决策提供有效支持；
- 满足法律、法规和合同的需要；
- 提供改善 ISMS 的机会。

信息安全体系审核可分为两种，一是内部信息安全管理体系审核，也称为一方审核，是组织的自我审核，其审核的目的是审核 ISMS 的符合性、有效性，采取纠正措施，使体系正常运行和持续改进；二是外部信息安全管理体系审核，也称第二方、第三方审核，其目的是选择合适的合作伙伴，证实合作方持续满足规定的要求，促进使用方改进信息安全管理体系。第二方审核是顾客对组织的审核，第三方审核是第三方性质的认证机构对申请认证的组织的审核。

5．管理评审

管理评审主要是指组织的最高管理者按规定的时间间隔对信息安全管理体系进行评审，以确保体系的持续适宜性、充分性和有效性。管理评审过程应确保收集到必要的信息，以供管理者进行评价，管理者评审应形成文件。

管理评审应根据信息安全管理体系审核的结果、环境的变化和对持续改进的承诺，指出可能需要修改的信息安全管理体系方针、策略、目标和其他要素。管理评审的评价结果是下一轮 PDCA 运行模式的开始。

管理评审与管理体系审核是不同的，管理评审的目的是确保 ISMS 体系持续的适宜性、充分性和有效性，而管理体系审核的目的是确保 ISMS 体系运行的符合性和有效性。

一般每年进行一次管理评审。有的认证机构会每半年有一次监督审核。发生某些情况时，应适时进行管理评审。具体情况包括：新的信息安全管理体系进入正式运行时；在第三方认证前；企业内、外部环境发生较大变化时，如组织结构、产品结构有重大调整，资源有重大改变，标准、法律、法规发生变更以及最高管理者认为必要时，如发生重大安全事故等。

6．趋势分析

趋势分析有助于组织识别需要改进的领域，并建立一个持续改进和循环提高的基础。

8.3.5 保持和改进 ISMS

通过监视和评审 ISMS，发现了组织 ISMS 体系运行中出现了不符合规定要求的事项后，就需要采取改进措施。

本阶段的主要工作有：测量信息安全管理体系满足安全方针和目标方面的业绩；识别信息安全管理体系的改进，并有效实施；采取适当的纠正和预防措施；沟通结果及活动，并与所有相关方磋商；必要时修订信息安全管理体系；确保修订达到预期的目标。下面介绍其中的几个关键问题：

1．不符合项的确定

一个不符合项是指：

- 缺少或缺乏有效地实施和维护一个或多个信息安全管理体系的要求；
- 在有客观证据的基础上，引起对信息安全管理体下完成信息安全方针和组织安全目标的能力的重大的怀疑。

不符合项一般是由以下原因形成的：

- 文件规定不符合标准（该说的没说到）；
- 现状不符合文件规定（说到的没做到）；
- 效果不符合规定要求（做到的没有效果）。

不符合项按不符合的程度可以分为：严重不符合、轻微不符合、观察项三类。

2．纠正性措施

组织应采取措施，消除不合格的、与实施和运行信息安全管理体系有关的原因，防止问题的再度发生。对纠正措施应该编制形成文件，确保以下要求：

- 识别实施和运行信息安全管理体系的不合格事件；
- 确定不合格的原因；
- 评价确保不合格不再发生的措施的需求；
- 确定和实施所需的纠正措施；
- 记录所采取措施的结果；
- 评审所采取的纠正措施。

3．预防性措施

组织应针对未来的安全事件确定预防措施以防止其发生。预防措施应与潜在问题的影响程度相适应。应为预防措施编制文件，以确定以下方面的需求：

- 识别潜在的不合格事件及其原因；
- 确定和实施所需的预防措施；
- 记录所采取措施的结果；
- 评审所采取的预防措施；识别已变更的风险并确保注意力关注在重大的已变更的风

险上；

- 纠正措施的优先权应以风险评估的结果为基础。

8.4 信息安全风险评估

本书2.1节介绍了信息系统的安全要素，连接这些要素与信息安全之间关系的纽带是“风险”。所谓的安全的信息系统，是指经过风险评估并对风险进行处理后，系统中残余的风险从可能产生的损失与预计的安全投入角度分析后被认为可以接受的系统。在此后几个章节的等级保护、信息系统安全工程以及信息安全管理体系等内容的介绍中，也多次提到风险评估的概念，它已经成为各种宏观的信息系统安全保护方案的方法学基础，例如，信息系统安全工程（ISSE）在发掘信息保护需求的阶段，便利用了风险评估的思想。而无论采用什么方法，都是一种在风险评估的基础上对风险进行处理的工程，这统称为风险管理。

风险管理的实质是基于风险的信息安全管理，即始终以风险为主线进行信息安全的管理。本章对国家标准 GB/T 20984-2007《信息安全技术 信息安全风险评估规范》中给出的风险评估基础知识作了介绍，实际上是对本章前三节的知识进行了升华。因为，ISO/IEC 27002 中的任何一项信息安全管理的控制措施，都针对的是系统中可能存在的风险点。而建立 ISMS 的过程，就是对安全风险进行评估，继而从 ISO/IEC 27002 中选择合适的信息安全管理控制措施的具体实践。

8.4.1 概述

信息安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，为防范和化解信息安全风险，将风险控制在可接受的水平，从而最大限度地保障信息安全提供科学依据。

本书 2.1 节已经介绍了信息系统的各个安全要素，并指出了这些安全要素之间的关系，本章就不再赘述。下面对风险分析的原理和风险评估的步骤进行说明。

1．风险分析

风险分析是风险评估的核心部分，是定量或定性计算安全风险的过程。

风险分析原理如图 8-5 所示。

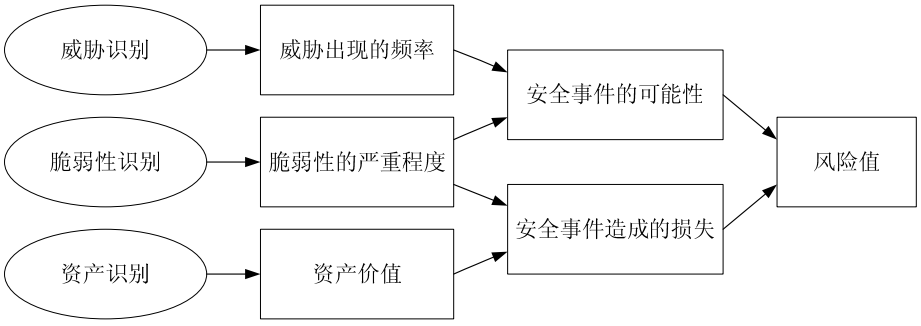


图 8-5　风险分析原理图

风险分析中要涉及资产、威胁、脆弱性三个基本要素。每个要素有各自的属性，资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。风险分析的主要内容为：

（1）对资产进行识别，并对资产的价值进行赋值；

（2）对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值；

（3）对脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值；

（4）根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性；

（5）根据脆弱性的严重程度及安全事件所作用的资产的价值计算安全事件造成的损失；

（6）根据安全事件发生的可能性以及安全事件出现后的损失，计算安全事件一旦发生对组织的影响，即风险值。

2．风险评估实施流程

风险评估的实施流程如图 8-6 所示。该图提出了实施风险评估的主要步骤，包括威胁识别、资产识别、脆弱性级别、已有安全措施的确认、风险计算、风险处理等。后面几个小节将对关键步骤进行进一步说明。

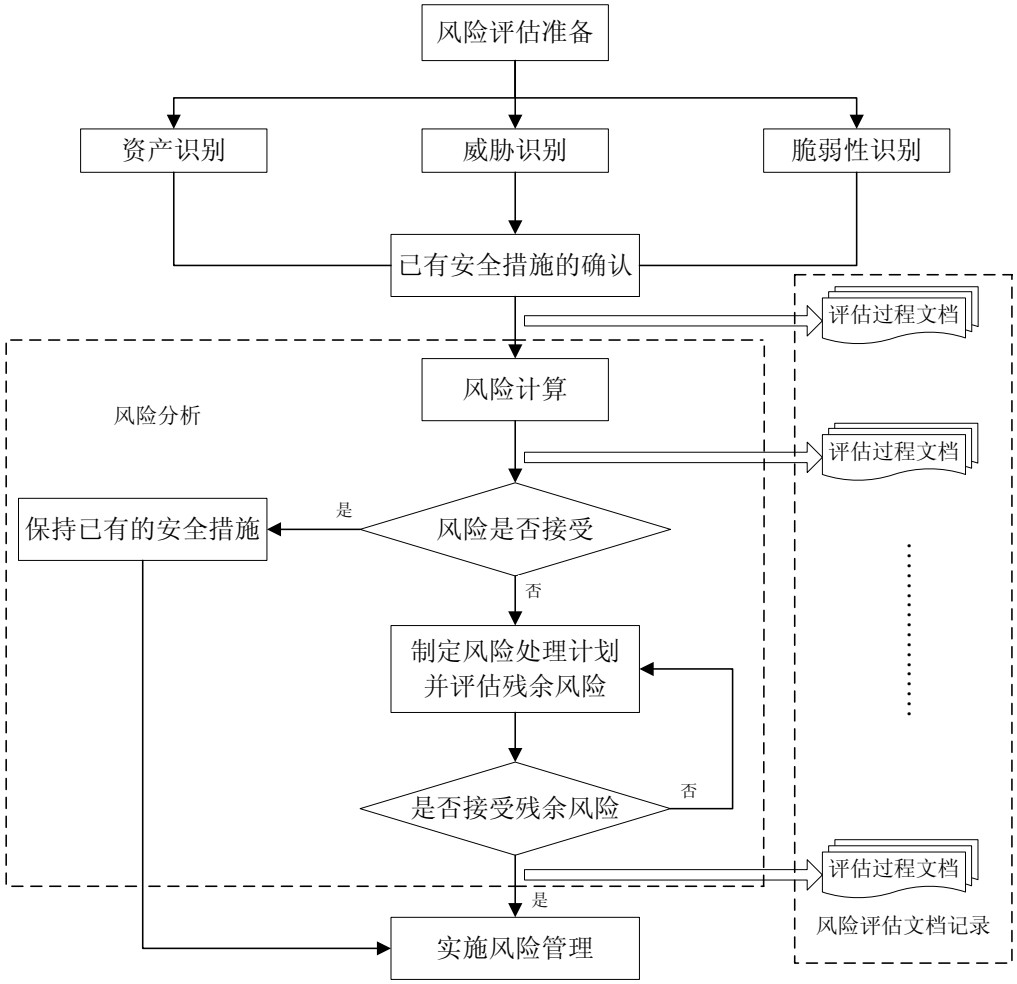


图 8-6　风险评估实施流程图

8.4.2　资产识别

保密性、完整性和可用性是评价资产的三个安全属性。风险评估中资产的价值不是以资产的经济价值来衡量，而是由资产在这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。安全属性达成程度的不同将使资产具有不同的价值，而资产面临的威胁、存在的脆弱性、以及已采用的安全措施都将对资产安全属性的达成程度产生影响。为此，应对组织中的资产进行识别。

资产识别的首先工作是对资产进行分类，然后需要对每项资产的保密性、完整性和可用性进行赋值，在此基础上评价资产的重要性。

1．资产分类

在一个组织中，资产有多种表现形式；同样的两个资产也因属于不同的信息系统而重要性不同，而且对于提供多种业务的组织，其支持业务持续运行的系统数量可能更多。这时首先需要将信息系统及相关的资产进行恰当的分类，以此为基础进行下一步的风险评估。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估者灵活把握。根

据资产的表现形式，可将资产分为数据、软件、硬件、服务、人员等类型。具体可参考 8.2.3 节的有关内容。

2．资产赋值

根据资产在保密性上的不同要求，将其分为五个不同的等级，分别对应资产在保密性上应达成的不同程度或者保密性缺失时对整个组织的影响。表 8-1 提供了一种保密性赋值的参考。

表 8-1　资产保密性赋值表

赋值	标识	定义
5	很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成灾难性的损害。
4	高	包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害。
3	中等	组织的一般性秘密，其泄露会使组织的安全和利益受到损害。
2	低	仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成轻微损害。
1	很低	可对社会公开的信息，公用的信息处理设备和系统资源等。

根据资产在完整性上的不同要求，将其分为五个不同的等级，分别对应资产在完整性上缺失时对整个组织的影响。表 8-2 提供了一种完整性赋值的参考。

表 8-2　资产完整性赋值表

赋值	标识	定义
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补。
4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，较难弥补。
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但可以弥补。
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，对业务冲击轻微，容易弥补。
1	很低	完整性价值非常低，未经授权的修改或破坏对组织造成的影响可以忽略，对业务冲击可以忽略。

根据资产在可用性上的不同要求，将其分为五个不同的等级，分别对应资产在可用性上应达成的不同程度。表 8-3 提供了一种可用性赋值的参考。

表 8-3　资产可用性性赋值表

赋值	标识	定义
5	很高	可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度 99.9%以上，或系统不允许中断。
4	高	可用性价值较高，合法使用者对信息及信息系统的可用度达到每天 90%以上，或系统允许中断时间小于 10min。
3	中等	可用性价值中等，合法使用者对信息及信息系统的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于 30min。
2	低	可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60min。
1	很低	可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%。

3．资产重要性等级

资产价值应依据资产在保密性、完整性和可用性上的赋值等级，经过综合评定得出。综合评定方法可以根据自身的特点，选择对资产保密性、完整性和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果；也可以根据资产保密性、完整性和可用性的不同等级对其赋值进行加权计算得到资产的最终赋值结果。加权方法可根据组织的业务特点确定。

国家标准中，为与上述安全属性的赋值相对应，根据最终赋值将资产划分为五级，级别越高表示资产越重要，也可以根据组织的实际情况确定资产识别中的赋值依据和等级。表 8-4 中的资产等级划分表明了不同等级的重要性的综合描述。评估者可根据资产赋值结果，确定重要资产的范围，并主要围绕重要资产进行下一步的风险评估。

表 8-4　资产等级及含义描述

等级	标识	描述

5	很高	非常重要，其安全属性破坏后可能对组织造成非常严重的损失。
4	高	重要，其安全属性破坏后可能对组织造成比较严重的损失。
3	中等	比较重要，其安全属性破坏后可能对组织造成中等程度的损失。
2	低	不太重要，其安全属性破坏后可能对组织造成较低的损失。
1	很低	不重要，其安全属性破坏后对组织造成导很小的损失，甚至忽略不计。

8.4.3 威胁识别

威胁是一个具有多种属性的信息安全要素，例如威胁主体、资源、动机、途径等属性，对其各个属性的了解，有助于提高对抗威胁的针对性，例如消除威胁的动机、增大威胁的资源消耗、切断威胁的途径（例如外部联网）等。因此，在识别威胁的过程中，重要的一个步骤是对威胁进行分类。此外，为了计算最终的风险值，还应对威胁赋值，描述威胁的严重性。

1．威胁分类

造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗的因素和其它物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，在保密性、完整性和可用性等方面造成损害；也可能是偶发的、或蓄意的事件。

在对威胁进行分类前，应考虑威胁的来源。表 8-5 提供了一种威胁来源的分类方法。

表 8-5　威胁来源列表

来源		描述
环境因素		断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震、意外事故等环境危害或自然灾害，以及软件、硬件、数据、通讯线路等方面的故障。
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；采用自主或内外勾结的方式盗窃机密信息或进行篡改，获取利益。 外部人员利用信息系统的脆弱性，对网络或系统的保密性、完整性和可用性进行破坏，以获取利益或炫耀能力。
	非恶意人员	内部人员由于缺乏责任心，或者由于不关心或不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致信息系统故障或被攻击。

对威胁进行分类的方式有多种，针对上表的威胁来源，可以根据其表现形式将威胁主要分为如表 8-6 所示的几类。在这一分类的基础上，评估者还应进一步刻画各类威胁的属性。

表 8-6　一种基于表现形式的威胁分类表

种类	描述	威胁子类
软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障等。
物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等。
无作为或操作失误	应该执行而没有执行相应的操作，或无意执行了错误的操作	维护错误、操作失误等。
管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行	管理制度和策略不完善、管理规程缺失、职责不明确、监督控管机制不健全等。
恶意代码	故意在计算机系统上执行恶意任务的程序代码	病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等。
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出破坏信息系统的行为	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等。
网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、嗅探（账号、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等。
物理攻击	通过物理的接触造成对软件、硬件、数据的破坏	物理接触、物理破坏、盗窃等。
泄密	信息泄露给不应了解的他人	内部信息泄露、外部信息泄露等。
篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等。
抵赖	不承认收到的信息和所作的操作和交易	原发抵赖、接收抵赖、第三方抵赖等。

2．威胁赋值

判断威胁出现的频率是威胁赋值的基本内容，评估者应根据经验和有关的统计数据来进行判断。在评估中，需要综合考虑以下三个方面：以往安全事件报告中出现过的威胁及其频率的统计；实际环境中通过检测工具以及各种日志发现的威胁及其频率的统计；近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。

可以对威胁出现的频率进行等级化处理，不同等级分别代表威胁出现的频率的高低。等级数值越大，威胁出现的频率越高。

表 8-7 提供了威胁出现频率的一种赋值方法。在实际的评估中，威胁频率的判断依据应在评估准备阶段根据历史统计或行业判断予以确定，并得到被评估方的认可。

表 8-7　威胁赋值表

等级	标识	定义
5	很高	出现的频率很高（或≥1 次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过。
4	高	出现的频率较高（或≥ 1 次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过。
3	中等	出现的频率中等（或〉1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过。
2	低	出现的频率较小；或一般不太可能发生；或没有被证实发生过。
1	很低	威胁几乎不可能发生；仅可能在非常罕见和例外的情况下发生。

8.4.4　脆弱性识别

如本书第 2 章所述，脆弱性的一个重要特点是，它是资产本身存在的，如果没有被相应的威胁利用，单纯的脆弱性本身不会对资产造成损害。而且如果系统足够强健，严重的威胁也不会导致安全事件发生，并造成损失。即，威胁总是要利用资产的脆弱性才可能造成危害。

脆弱性识别是风险评估中最重要的一个环节。脆弱性识别可以以资产为核心，针对每一项需要保护的资产,识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估；也可以从物理、网络、系统、应用等层次进行识别，然后与资产、威胁对应起来。脆弱性识别的依据可以是国际或国家安全标准，也可以是行业规范、应用流程的安全要求。对应用在不同环境中的相同的弱点，其脆弱性严重程度是不同的，评估者应从组织安全策略的角度考虑、判断资产的脆弱性及其严重程度。信息系统所采用的协议、应用流程的完备与否、与其他网络的互联等也应考虑在内。

资产的脆弱性具有隐蔽性，有些脆弱性只有在一定条件和环境下才能显现，这是脆弱性识别中最为困难的部分。不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个脆弱性。

1．脆弱性识别的内容

脆弱性识别时需要掌握的数据应来自于资产的所有者、使用者，以及相关业务领域和软硬件方面的专业人员等。脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。

脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题。管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关。

对不同的识别对象，其脆弱性识别的具体要求应参照相应的技术或管理标准实施。例如，对物理环境的脆弱性识别可按 GB/T 9361-2000《计算机场地安全要求》中的技术指标实施；对管理脆弱性识别可按 GB/T 22081-2008《信息技术 安全技术 信息安全管理实用规则》的要求对安全管理制度及其执行情况进行检查，发现管理脆弱性和不足；对技术脆弱性的识别则比较复杂，除了参照有关标准外，还要特别注意有关国际组织和产品厂商发布了漏洞信息。表 8-8 提供了一种脆弱性识别内容的参考。

表 8-8　脆弱性识别内容表

类型	识别对象	识别内容

技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别。
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别。
	系统软件	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面进行识别。
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别。
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密码保护等方面进行识别。
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别。
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别。

2．脆弱性赋值

可以根据脆弱性对资产的暴露程度、技术实现的难易程度、流行程度等，采用等级方式对已识别的脆弱性的严重程度进行赋值。由于很多脆弱性反映的是同一方面的问题，或可能造成相似的后果，赋值时应综合考虑这些脆弱性，以确定这一方面脆弱性的严重程度。

对某个资产，其技术脆弱性的严重程度还受到组织管理脆弱性的影响。因此，资产的脆弱性赋值还应参考技术管理和组织管理脆弱性的严重程度。

脆弱性严重程度可以进行等级化处理，不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度越高。表 8-9 提供了脆弱性严重程度的一种赋值方法。

表 8-9　脆弱性严重程度赋值表

等级	标识	定义
5	很高	如果被威胁利用，将对资产造成完全损害。
4	高	如果被威胁利用，将对资产造成重大损害。
3	中等	如果被威胁利用，将对资产造成一般损害。
2	低	如果被威胁利用，将对资产造成较小损害。
1	很低	如果被威胁利用，将对资产造成的损害可以忽略。

8.4.5　风险分析与处理

风险分析是根据资产识别、威胁识别和脆弱性级别的结果，计算实际的风险值。风险分析工作中，还要对现有安全措施进行评价，在此基础上提出对风险处置的具体建议。严格而言，风险处置的具体行为并不是风险评估的组成部分，但它们共同组成了风险管理活动。

1．风险计算原理

在计算风险时，需要综合安全事件所作用的资产的价值及脆弱性的严重程度，判断安全事件对组织的影响。以下面的范式形式化加以说明风险的计算原理：

风险值 ＝R（A，T，V）＝R（L（T，V），F（Ia，Va））。

其中，R 表示安全风险计算函数；A 表示资产；T 表示威胁；V 表示脆弱性；Ia 表示安全事件所作用的资产价值；Va 表示脆弱性严重程度；L 表示威胁利用资产的脆弱性导致安全事件的可能性；F 表示安全事件发生后造成的损失。这个公式有以下三个关键计算环节：

（1）计算安全事件发生的可能性

根据威胁出现频率及脆弱性的状况，计算威胁利用脆弱性导致安全事件发生的可能性，即：

安全事件的可能性 ＝L（威胁出现频率，脆弱性）＝ L（T，V ）。

在具体评估中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识的公开程度等）、资产吸引力等因素来判断安全事件发生的可能性。

（2）计算安全事件发生后造成的损失

根据资产价值及脆弱性严重程度，计算安全事件一旦发生后造成的损失，即：

安全事件造成的损失 ＝F（资产价值，脆弱性严重程度）＝ F（Ia，Va）。

部分安全事件的发生造成的损失不仅仅是针对该资产本身，还可能影响业务的连续性；

不同安全事件的发生对组织的影响也是不一样的。在计算某个安全事件的损失时，应将对组织的影响也考虑在内。

部分安全事件造成的损失的判断还应参照安全事件发生可能性的结果，对发生可能性极小的安全事件，如处于非地震带的地震威胁、在采取完备供电措施状况下的电力故障威胁等，可以不计算其损失。

（3）计算风险值

根据计算出的安全事件的可能性以及安全事件造成的损失，计算风险值，即：

风险值 ＝R（安全事件的可能性，安全事件造成的损失）＝ R（L（T，V），F（Ia，Va））。

评估者可根据自身情况选择相应的风险计算函数计算风险值，如矩阵法或相乘法。矩阵法通过构造一个二维矩阵，形成安全事件的可能性与安全事件造成的损失之间的二维关系；相乘法通过构造经验函数，将安全事件的可能性与安全事件造成的损失进行运算得到风险值。

2．风险结果判定

为实现对风险的控制与管理，可以对风险评估的结果进行等级化处理。可将风险划分为五级，等级越高，风险越高。

评估者应根据所采用的风险计算方法，计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表了相应风险的严重程度。

表 8-10 提供了一种风险等级划分方法。

表 8-10　风险等级划分表

等级	标识	描述
5	很高	一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏、严重影响组织的正常经营，经济损失重大、社会影响恶劣。
4	高	一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害。
3	中等	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大。
2	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段很快能解决。
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补。

3．风险处理

风险等级处理的目的是为了在风险管理过程中对不同风险实现直观比较，以确定组织的安全策略。组织应当综合考虑风险控制成本与风险造成的影响，提出一个可接受的风险范围。对某些资产的风险，如果风险计算值在可接受的范围内，则该风险是可接受的，应保持已有的安全措施；如果风险评估值在可接受的范围外，即风险计算值高于可接受范围的上限值，则该风险是不可接受的，需要采取安全措施以降低、控制风险。另一种确定不可接受的风险的办法是根据等级化处理的结果，不设定可接受风险值的基准，对达到相应等级的风险都进行处理。

对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划。风险处理计划中应明确采取的弥补脆弱性的安全措施、预期效果、实施条件、进度安排、责任部门等。安全措施的选择应从管理与技术两个方面考虑。安全措施的选择与实施应参照信息安全的相关标准进行。这与本书第 2 章所述的信息安全风险控制是同样的概念。如同第 2 章所述，在处理不可接受的风险时，还可采取风险规避和风险转移措施。

在对于不可接受的风险选择适当安全措施后，为确保安全措施的有效性，可进行再评估，以判断实施安全措施后的残余风险是否已经降低到可接受的水平。残余风险的评估可以依据常规的风险评估流程实施，也可做适当裁减。一般来说，安全措施的实施是以减少脆弱性或降低安全事件发生可能性为目标的，因此，残余风险的评估可以从脆弱性评估开始，在对照

安全措施实施前后的脆弱性状况后，再次计算风险值的大小。这也说明，风险评估是一个不断循环往复的过程，且风险应该处在不断的监视之中。

8.4.6 风险评估与信息系统生命周期阶段的关系

风险评估应贯穿于信息系统生命周期的各阶段中。信息系统生命周期各阶段涉及的风险评估的原则和方法是一致的，但由于各阶段实施的内容、对象、安全需求不同，使得风险评估的对象、目的、要求等各方面也有所不同。具体而言，在规划设计阶段，通过风险评估以确定系统的安全目标；在建设验收阶段，通过风险评估以确定系统的安全目标达成与否；在运行维护阶段，要不断地实施风险评估以识别系统面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现。因此，每个阶段风险评估的具体实施应根据该阶段的特点有所侧重地进行。有条件时，应采用风险评估工具开展风险评估活动。

1．规划阶段的风险评估

规划阶段风险评估的目的是识别系统的业务战略，以支撑系统安全需求及安全战略等。规划阶段的评估应能够描述信息系统建成后对现有业务模式的作用，包括技术、管理等方面，并根据其作用确定系统建设应达到的安全目标。

本阶段评估中，资产、脆弱性不需要识别；威胁应根据未来系统的应用对象、应用环境、业务状况、操作要求等方面进行分析。评估着重在以下几方面：

- 是否依据相关规则，建立了与业务战略相一致的信息系统安全规划，并得到最高管理者的认可；
- 系统规划中是否明确信息系统开发的组织、业务变更的管理、开发优先级；
- 系统规划中是否考虑信息系统的威胁、环境，并制定总体的安全方针；
- 系统规划中是否描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；
- 系统规划中是否描述所有与信息系统安全相关的运行环境，包括物理和人员的安全配置，以及明确相关的法规、组织安全策略、专门技术和知识等。

规划阶段的评估结果应体现在信息系统整体规划或项目建议书中。

2．设计阶段的风险评估

设计阶段的风险评估需要根据规划阶段所明确的系统运行环境、资产重要性，提出安全功能需求。设计阶段的风险评估结果应对设计方案中所提供的安全功能符合性进行判断，作为采购过程风险控制的依据。

本阶段评估中，应详细评估设计方案中对系统面临威胁的描述，将使用的具体设备、软件等资产列表，以及这些资产的安全功能需求。对设计方案的评估着重在以下几方面：

- 设计方案是否符合系统建设规划，并得到最高管理者的认可；
- 设计方案是否对系统建设后面临的威胁进行了分析，重点分析来自物理环境和自然的威胁，以及由于内、外部入侵等造成的威胁；
- 设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析，制定信息系统的总体安全策略；
- 设计方案是否采取了一定的手段来应对系统可能的故障；
- 设计方案是否对设计原型中的技术实现以及人员、组织管理等方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性；
- 设计方案是否考虑随着其他系统接入而可能产生的风险；
- 系统性能是否满足用户需求，并考虑到峰值的影响，是否在技术上考虑了满足系统性能要求的方法；
- 应用系统（含数据库）是否根据业务需要进行了安全设计；
- 设计方案是否根据开发的规模、时间及系统的特点选择开发方法，并根据设计开发

计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

- 设计活动中所采用的安全控制措施、安全技术保障手段对风险的影响。在安全需求变更和设计变更后，也需要重复这项评估。

设计阶段的评估可以以安全建设方案评审的方式进行，判定方案所提供的安全功能与信息技术安全技术标准的符合性。评估结果应体现在信息系统需求分析报告或建设实施方案中。

3．实施阶段的风险评估

实施阶段风险评估的目的是根据系统安全需求和运行环境对系统开发、实施过程进行风险识别，并对系统建成后的安全功能进行验证。根据设计阶段分析的威胁和制定的安全措施，在实施及验收时进行质量控制。

基于设计阶段的资产列表、安全措施，实施阶段应对规划阶段的安全威胁进行进一步细分，同时评估安全措施的实现程度，从而确定安全措施能否抵御现有威胁、脆弱性的影响。实施阶段风险评估主要对系统的开发与技术/产品获取、系统交付实施两个过程进行评估。

开发与技术/产品获取过程的评估要点包括：

- 法律、政策、适用标准和指导方针：直接或间接影响信息系统安全需求的特定法律；影响信息系统安全需求、产品选择的政府政策、国际或国家标准；
- 信息系统的功能需要：安全需求是否有效地支持系统的功能；
- 成本效益风险：是否根据信息系统的资产、威胁和脆弱性的分析结果，确定在符合相关法律、政策、标准和功能需要的前提下选择最合适的安全措施；
- 评估保证级别：是否明确系统建设后应进行怎样的测试和检查，从而确定是否满足项目建设、实施规范的要求。

系统交付实施过程的评估要点包括：

- 根据实际建设的系统，详细分析资产、面临的威胁和脆弱性；
- 根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁；
- 评估是否建立了与整体安全策略一致的组织管理制度；
- 对系统实现的风险控制效果与预期设计的符合性进行判断，如存在较大的不符合，应重新进行信息系统安全策略的设计与调整。

本阶段风险评估可以采取对照实施方案和标准要求的方式，对实际建设结果进行测试、分析。

4．运行维护阶段的风险评估

运行维护阶段风险评估的目的是了解和控制运行过程中的安全风险，是一种较为全面的风险评估。评估内容包括对真实运行的信息系统、资产、威胁、脆弱性等各方面。

- 资产评估：在真实环境下较为细致的评估。包括实施阶段采购的软硬件资产、系统运行过程中生成的信息资产、相关的人员与服务等，本阶段资产识别是前期资产识别的补充与增加；
- 威胁评估：应全面地分析威胁的可能性和影响程度。对非故意威胁导致安全事件的评估可以参照安全事件的发生频率；对故意威胁导致安全事件的评估主要就威胁的各个影响因素做出专业判断；
- 脆弱性评估：是全面的脆弱性评估。包括运行环境中物理、网络、系统、应用、安全保障设备、管理等各方面的脆弱性。技术脆弱性评估可以采取核查、扫描、案例验证、渗透性测试的方式实施；安全保障设备的脆弱性评估，应考虑安全功能的实现情况和安全保障设备本身的脆弱性；管理脆弱性评估可以采取文档、记录核查等方式进行验证；

- 风险计算：根据本标准的相关方法，对重要资产的风险进行定性或定量的风险分析，描述不同资产的风险高低状况。

运行维护阶段的风险评估应定期执行；当组织的业务流程、系统状况发生重大变更时，也应进行风险评估。重大变更包括以下情况（但不限于）：

- 增加新的应用或应用发生较大变更；
- 网络结构和连接状况发生较大变更；
- 技术平台大规模的更新；
- 系统扩容或改造；
- 发生重大安全事件后，或基于某些运行记录怀疑将发生重大安全事件；
- 组织结构发生重大变动对系统产生了影响。

5．废弃阶段的风险评估

当信息系统不能满足现有要求时，信息系统进入废弃阶段。根据废弃的程度，又分为部分废弃和全部废弃两种。

废弃阶段风险评估着重在以下几方面：

- 确保硬件和软件等资产及残留信息得到了适当的处置，并确保系统组件被合理地丢弃或更换；
- 如果被废弃的系统是某个系统的一部分，或与其他系统存在物理或逻辑上的连接，还应考虑系统废弃后与其他系统的连接是否被关闭；
- 如果在系统变更中废弃，除对废弃部分外，还应对变更的部分进行评估，以确定是否会增加风险或引入新的风险；
- 是否建立了流程，确保更新过程在一个安全、系统化的状态下完成。

本阶段应重点对废弃资产对组织的影响进行分析，并根据不同的影响制定不同的处理方式。对由于系统废弃可能带来的新的威胁进行分析，并改进新系统或管理模式。对废弃资产的处理过程应在有效的监督之下实施，同时对废弃的执行人员进行安全教育。

信息系统的维护技术人员和管理人员均应该参与此阶段的评估。

本章小结

本章集中介绍了信息安全管理的知识。虽然这只是本书若干章节中的一节，但信息安全管理的重要性却是如何强调都不过分的。在信息安全管理的基础知识之外，本章还提供了有关风险评估的知识，这些知识构成了各种信息系统安全保护方法的原理基础，它们也更有助于更好地理解“信息安全工程”一章中描述的信息系统安全工程过程。

本章主要内容有：

（1）信息安全管理的基础知识（概述）

信息安全管理是指把分散的信息安全技术因素和人的因素，通过策略、规则协调整合成为一体，服务于信息安全的目标。信息安全管理之所以重要，一方面是因为仅仅依靠技术和产品保障信息安全是不够的，另一方面则是实际发生的信息安全事件的统计数据证明，有95%的事件可以通过科学的信息安全管理来避免。

近年来，信息安全管理标准发展迅速。国外于此有关的标准有 BS 7799 标准、ISO/IEC 17799 标准、ISO/IEC 2700X 系列标准、ISO/IEC TR 13335 标准、信息及相关技术控制目标（COBIT）、IT 服务流程管理（ITIL）等。国内则主要转化了上述的部分有关国际标准，且参照上述标准制定了 GB/T 20269-2006《信息安全技术 信息系统安全管理要求》和 GB/T 20282-2006《信息安全技术 信息系统安全工程管理要求》。

（2）信息安全管理控制措施

为了对组织所面临的信息安全风险实施有效的控制，组织要针对具体的安全威胁和薄弱

点采取适当的控制措施，包括管理手段和技术方法。根据 ISO/IEC 27002 标准，本章详细介绍了 11 个方面的管理控制措施，包括信息安全方针，信息安全组织，资产管理，人力资源安全，物理和环境安全，通信和操作管理，访问控制，信息系统获取、开发和维护，信息安全事件管理，业务连续性管理以及符合性。

（3）信息安全管理体系

信息安全管理体系 ISMS 是组织基于业务风险方法，建立、实施、运行、监视、评审、保持和改进信息安全的体系，是一个组织整个管理体系的一部分，它包括组织结构、方针策略、规划活动、职责、实践、规程、过程和资源。当前，以 ISO/IEC2700X 为基础，建立信息安全管理体系（ISMS），已经成为很多组织开展信息系统安全建设的基本方法。

ISMS 基于 PDCA 循环，将安全管理的计划、实施、检查和改进 4 个环节链接成一个环状的循环过程。建立一个 ISMS 包含确定信息安全政策、确定 ISMS 的范围、实施风险评估、管理风险、选择控制目标和控制对象、适用性声明等部分。基于 PDCA 的理论，信息安全管理体系相关工作还包括实施和运行 ISMS、监视和评审 ISMS 以及保持和改进 ISMS。

（4）信息安全风险评估

信息安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，为防范和化解信息安全风险，将风险控制在可接受的水平，从而最大限度地保障信息安全提供科学依据。风险评估实施流程包括威胁识别、资产识别、脆弱性级别、已有安全措施的确认、风险计算、风险处理等过程。

风险评估贯穿于信息系统生命周期的各阶段中。各阶段涉及的风险评估的原则和方法是一致的，但由于各阶段实施的内容、对象、安全需求不同，使得风险评估的对象、目的、要求等各方面也有所不同。

习题

1．什么是信息安全管理？概述信息安全管理的必要性。
2．国际上有哪些主要的信息安全管理标准？我国已制订的信息安全管理标准有哪些？
3．信息安全管理控制措施主要涉及哪些方面的管理措施？
4．概述信息安全组织的主要管理措施。
5．概述资产管理的主要管理措施。
6．概述访问控制的主要管理措施。
7．概述信息系统获取、开发和维护过程中的主要管理措施。
8．概述通信与操作管理的主要管理措施。
9．什么是 PDCA 模型？它有什么特点？
10．概述建立信息安全管理体系（ISMS）的过程。
11．风险评估的重要意义是什么？
12．概述风险评估的实施流程。
13．风险评估在信息系统生命周期各阶段的作用是什么？

第 9 章　信息安全应急处理和灾难恢复

本章要点

- 信息安全事件分类分级标准
- 信息安全应急处理关键过程
- 信息系统灾难恢复能力等级划分
- 信息系统灾难恢复需求确定
- 信息系统灾难恢复策略

9.1　信息安全事件分类

信息安全事件指由于自然或者人为的原因，对信息系统造成危害，或在信息系统内发生对社会造成负面影响的事件。本节和下一节以国家标准 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》为基础，分别介绍了信息安全事件分类和分级的有关知识。

9.1.1　考虑要素与基本分类

对信息安全事件分类的主要依据是信息安全事件发生的原因、表现形式等因素。

根据上述考虑，国家标准 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》将信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其它信息安全事件等 7 个基本分类，每个基本分类分别包括若干个子类。

9.1.2　有害程序事件

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序，有害程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行。

有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等 7 个子类。

（1）计算机病毒事件是指蓄意制造、传播计算机病毒，或是因受到计算机病毒影响而导致的信息安全事件。计算机病毒是指编制或者在计算机程序中插入的一组计算机指令或者程序代码，它可以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。

（2）蠕虫事件是指蓄意制造、传播蠕虫，或是因受到蠕虫影响而导致的信息安全事件。蠕虫是指除计算机病毒以外，利用信息系统缺陷，通过网络自动复制并传播的有害程序。

（3）特洛伊木马事件是指蓄意制造、传播特洛伊木马程序，或是因受到特洛伊木马程序影响而导致的信息安全事件。特洛伊木马程序是指伪装在信息系统中的一种有害程序，具有控制该信息系统或进行信息窃取等对信息系统有害的功能。

（4）僵尸网络事件是指利用僵尸工具软件，形成僵尸网络而导致的信息安全事件。僵尸网络是指网络上受到黑客集中控制的一群计算机，它可以被用于伺机发起网络攻击，进行信息窃取或传播木马、蠕虫等其它有害程序。

（5）混合攻击程序事件是指蓄意制造、传播混合攻击程序，或是因受到混合攻击程序影响而导致的信息安全事件。混合攻击程序是指利用多种方法传播和感染其它系统的有害程序，可能兼有计算机病毒、蠕虫、木马或僵尸网络等多种特征。混合攻击程序事件也可以是

一系列有害程序综合作用的结果，例如一个计算机病毒或蠕虫在侵入系统后安装木马程序等。

（6）网页内嵌恶意代码事件是指蓄意制造、传播网页内嵌恶意代码，或是因受到网页内迁恶意代码影响而导致的信息安全事件。网页内迁恶意代码是指内嵌在网页中，未经允许由浏览器执行，影响信息系统正常运行的有害程序。

（7）其它有害程序事件是指不能包含在以上 6 个子类之中的有害程序事件。

9.1.2 网络攻击事件

网络攻击事件是指通过网络或其它技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。

网络攻击事件网络攻击包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其它网络攻击事件等 7 个子类。

（1）拒绝服务攻击事件是指利用信息系统缺陷、或通过暴力攻击的手段，以大量消耗信息系统的 CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行为目的的信息安全事件。

（2）后门攻击事件是指利用软件系统、硬件系统设计过程中留下的后门或者有害程序所设置的后门而对信息系统实施攻击的信息安全事件。

（3）漏洞攻击事件是指除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件。

（4）网络扫描窃听事件是指利用网络扫描或窃听软件，获取信息系统网络配置、端口、服务、存在的脆弱性等特征而导致的信息安全事件。

（5）网络钓鱼事件是指利用欺骗性的计算机网络技术，使用户泄露重要信息而导致的信息安全事件。例如，利用欺骗性的电子邮件获取用户银行帐号密码等。

（6）干扰事件是指通过技术手段对网络进行干扰，或对广播电视有线或无线传输网络进行插播，对卫星广播电视信号非法攻击等导致的信息安全事件。

（7）其它网络攻击事件是指不能被包含在以上 6 个子类之中的网络攻击事件。

9.1.3 信息破坏事件

信息破坏事件是指通过网络或其它技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。

信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件等 5 个子类。

（1）信息篡改事件是指未经授权将信息系统中的信息更换为攻击者所提供的异常信息而导致的信息安全事件，例如网页篡改等导致的信息安全事件。

（2）信息假冒事件是指通过假冒他人信息系统收发信息而导致的信息安全事件，例如网页假冒等导致的信息安全事件。

（3）信息泄漏事件是指因误操作或软硬件缺陷等因素导致信息系统中信息暴露于未经授权者而导致的信息安全事件。

（4）信息窃取事件是指未经授权用户利用可能的技术手段恶意主动获取信息系统中信息而导致的信息安全事件。

（5）信息丢失事件是指因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件。

（6）其它信息破坏与假冒事件是指不能被包含在以上 5 个子类之中的信息破坏事件。

9.1.4 信息内容安全事件

信息内容安全事件是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的

内容的安全事件。

信息内容安全事件包括以下 4 个子类。

（1）违反宪法和法律、行政法规的信息安全事件；

（2）针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；

（3）组织串连、煽动集会游行的信息安全事件；

（4）其它信息内容安全事件。

9.1.5 设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。

设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障等 4 个子类。

（1）软硬件自身故障是指因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的信息安全事件。

（2）外围保障设施故障是指由于保障事发组织信息系统正常运行所必须的外部设施出现故障而导致的信息安全事件，例如电力故障、外围网络故障等导致的信息安全事件。

（3）人为破坏事故是指人为的使用非技术手段，蓄意地对保障信息系统正常运行的硬件、软件实施窃取、破坏造成的信息安全事件；或由于人为的遗失、误操作以及其它无意行为造成信息系统硬件、软件遭到破坏，影响信息系统正常运行的信息安全事件。

（4）其它设备设施故障是指不能被包含在以上 3 个子类之中的因设备设施故障而导致的信息安全事件。

9.1.6 灾害性事件

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。

灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

9.1.7 其它信息安全事件

其它信息安全事件类别是指不能归为以上 6 个基本分类的信息安全事件。

9.2 信息安全事件分级

9.2.1 分级考虑因素

对信息安全事件的分级可参考下列三个要素：信息系统的重要程度、系统损失和社会影响。

1．信息系统的重要程度

信息系统的重要程度主要考虑信息系统所承载的业务对国家安全、经济建设、社会生活的重要性，以及业务对信息系统的依赖程度，划分为特别重要信息系统、重要信息系统和一般信息系统。

2．系统损失

系统损失是指由于信息安全事件对信息系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失。

特别严重的系统损失是指造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对事发组织是不可承受的。

严重的系统损失是指造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对事发组织是可承受的。

较大的系统损失是指造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对事发组织是完全可承受的。

较小的系统损失是指造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

3．社会影响

社会影响是指信息安全事件对社会所造成影响的范围和程度，其大小主要考虑国家安全、社会秩序、经济建设和公众利益等方面的影响。可将社会影响分为特别重大的社会影响、重大的社会影响、较大的社会影响和一般的社会影响。

特别重大的社会影响是指涉及到一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益。

重大的社会影响是指涉及到一个或多个地市的大部分地区，威胁到国家安全，引起社会恐慌，对经济建设有重大的负面影响，或者损害到公众利益。

较大的社会影响是指涉及到一个或多个地市的部分地区，可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益。

一般的社会影响是指涉及到一个地市的部分地区，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害。

根据上述的信息安全事件分级参考要素，将信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件。

9.2.2 特别重大事件（Ⅰ级）

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要信息系统遭受特别重大的系统损失。

（2）会产生特别重大的社会影响。

9.2.3 重大事件（Ⅱ级）

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要信息系统遭受重大的系统损失，或使重要信息系统遭受特别重大的系统损失。

（2）产生重大的社会影响。

9.2.4 较大事件（Ⅲ级）

较大事件是指能够导致较严重影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要信息系统遭受较大的系统损失，或使重要信息系统遭受重大的系统损失、一般信息信息系统遭受特别重大的系统损失。

（2）产生较大的社会影响。

9.2.5 一般事件（Ⅳ级）

一般事件是指能够导致较小影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要信息系统遭受较小的系统损失，或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失。

（2）产生一般的社会影响。

9.3 信息安全应急处理关键过程

信息安全应急处理指通过制定应急计划使得影响信息系统安全的安全事件能够得到及时响应，并在安全事件一旦发生后进行标识、记录、分类和处理，直到受影响的业务恢复正常运行的过程。这里的安全事件是 9.1 节列举的有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其它信息安全事件等七类事件。

信息安全应急处理是保障业务连续性的重要手段之一，是在处理信息安全事件时提供紧急现场或远程援助的一系列技术的和非技术的措施和行动，以降低安全事件给用户造成的损失或影响，涵盖了在安全事件发生后为了维持和恢复关键的应用所进行的系列活动。

与应急处理服务容易发生混淆的是灾难恢复服务，灾难恢复服务指的是将信息系统从灾难造成的故障或瘫痪状态恢复到可正常运行的状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态的活动和流程。与应急处理服务相比，灾难恢复服务的应用范围较窄，通常应用于重大的、特别是灾难性的、造成长时间无法访问正常设施的事件。9.4 节介绍了灾难恢复的有关内容。

本节分 6 个阶段，17 个主要安全控制点对信息安全应急处理的过程做了说明。

9.3.1 准备阶段

该阶段的目标是在事件真正发生之前为处理事件做好准备工作。准备阶段的主要工作包括建立合理的防御/控制措施、建立适当的策略和程序、获得必要的资源和组建响应队伍等。该阶段的控制点包括四个：应急响应需求界定、服务合同或协议签订、应急服务方案界定、人员和工具准备。

1．应急响应需求界定

在界定应急响应需求时，应首先了解各项业务功能及各项业务功能之间的相关性，确定支持各种业务功能的相应信息系统资源及其它资源，明确相关信息的保密性、完整性和可用性要求。

不论应急服务服务由组织自己提供，还是由外部提供，均应对信息系统进行全面评估，确定系统所执行关键功能，并确定执行这些功能所需的特定系统资源。此外，还应采用定量或定性的方法，对业务中断、系统宕机、网络瘫痪等突发信息安全事件造成的影响进行评估。

应急服务队伍应协助系统主管部门或运营部门建立合理的信息安全应急响应策略，该策略中应说明在业务中断、系统宕机、网络瘫痪等突发信息安全事件发生后，快速有效地恢复信息系统运行的方法。

2．服务合同或协议签订

如果应急影响服务由外部提供（一般而言，虽然各组织的信息技术部门有一定的应急响应能力，可以处理简单的事件，但仍需要与专业的信息安全服务组织签订应急响应服务合同，对处理重大事件做好准备），应急服务提供者应与服务对象签订应急服务合同或协议。在应急服务合同或协议中，应明确双方的职责和责任，指明哪些类型安全事件的应急响应行为需要系统管理者批准。此外，应急服务合同或协议应明确服务提供者的保密责任。

3．应急服务方案制定

应急服务提供者应在服务对象应急需求基础上制定服务方案。服务方案应根据业务影响分析的结果，明确应急响应的恢复目标，包括：

- 关键业务功能及恢复的优先顺序；
- 恢复时间范围，即恢复时间目标和恢复点目标的范围。

服务方案应带有完善的检测技术规范，检测技术规范至少应包含检测目的、工具、步骤等内容。常见的检测技术规范包括但不限于：

- Windows 系统检测技术规范；

- UNIX 系统检测技术规范；
- 数据库系统检测技术规范；
- 常用应用系统检测技术规范；
- 常见网络安全事件检测技术规范。

4．人员和工具准备

应急服务提供者应具有处理网络安全事件的工具包，包括常用的系统命令、工具软件等。这些工具包应保存在不可更改的移动介质上，如一次性可写光盘，此外还应定期更新。

应急响应工作需要大量的人力参与，特别是对一些重大事件的处理。因此服务提供者和信息系统运营单位应能随时调动一定数量的应急技术人员和辅助人员。

9.3.2 检测阶段

该阶段的目标是对信息安全事件做出初步的动作和响应，根据获得的初步材料和分析结果，预估事件的范围和影响程度，制定进一步的响应策略，并且保留相关证据。

该阶段的控制点包括三个：检测对象及范围确定、检测方案确定、检测实施。

1．检测对象及范围确定

应急技术人员应对发生异常的系统进行初步分析，判断是否真正发生了安全事件。

如果由外部组织提供应急响应服务，则外部的应急服务提供者应与信息系统运营者共同初步确定检测对象及范围，且检测对象及范围应得到服务对象的书面授权。

2．检测方案确定

如果由外部组织提供应急响应服务，则外部的应急服务提供者应与信息系统运营者共同确定检测方案。如果由组织自身提供应急影响服务，则也应制定检测方案并报经批准。

检测方案中应明确应急时所使用的检测规范，说明检测范围，并预测应急处理方案可能造成的影响。此外，检测方案还应包含实施方案失败的应变和回退措施。

发生信息安全事件时，往往情况非常紧急，可能没有时间制定完整、复杂的检测方案并经层层审批。在这种情况下，即使迫不得已以口头形式确定检测方案，应急技术人员也应与业务人员、管理人员等各方面相关人员做好沟通，

3．检测实施

确定检测方案后，应急技术人员应立即按照检测方案实施检测；

检测内容包含但不限于以下几个方面：

- 收集并记录系统信息，特别是在执行备份的过程中可能遗失或无法捕获的信息，如所有的当前网络连接；所有的当前进程；当前登陆的活动用户；所有打开了的文件，因为在断开网络连接时可能有些文件会被删除；其它所有容易丢失的数据，如内存和缓存中的数据；
- 备份被入侵的系统，至少应备份已确认被攻击了的系统及系统上的用户数据；
- 隔离被入侵的系统。把备份的文件传到一个与生产系统相隔离的测试系统上，并在测试系统上恢复被入侵系统,或者断开被破坏的系统并且直接在这些系统上进行分析；
- 查找其它系统上的入侵痕迹。其它系统包括同一 IP 地址段或同一网段的系统；处于同一域的其它系统；具有相同网络服务的系统；具有同一操作系统的系统；
- 检查防火墙、IDS 和路由器等设备的日志，分析哪些日志信息源于以前从未被注意到的系统连接或事件，并且确定哪些系统已经被攻击；
- 确定攻击者的入侵路径和方法。分析系统的本地日志，特别是入侵者试图猜测密码时的拒绝访问信息、与某些漏洞相关的信息、由 TCP Wrapper 等工具所收集的某些特定服务信息等，判断攻击者的入侵路径和方法；
- 确定入侵者进入系统后的行为。通过分析各种日志文件；将受攻击机器上的完整性

校验和和文件同已知的可信任的完整性校验和和文件进行比较；借用一些检测工具和分析工具等方式，确定入侵者是如何实施攻击并获得系统的访问权限的。

如果由外部组织实施检测，则应急服务提供者的检测工作应在系统运营者的监督与配合下完成。应急服务提供者应配合服务对象，将所检测到的安全事件向有关部门和人员通报或报告。

9.3.3 抑制阶段

抑制阶段的目标是限制攻击的范围，抑制潜在的或进一步的攻击和破坏。抑制措施十分重要，因为安全事件可能很容易扩散和失控。攻击抑制措施可以在以下几个方面发挥作用：阻止入侵者访问被攻陷系统；限制入侵的程度；防止入侵者进一步破坏等。

该阶段的控制点包括三个：抑制方法确定、抑制方法认可、抑制实施。

1．抑制方法确定

在检测分析的基础上，应急技术人员应迅速确定与安全事件相应的抑制方法。在确定抑制方法时，需要考虑：

- 全面评估入侵范围以及入侵带来的影响和损失；
- 通过分析得到的其它结论，例如入侵者的来源；
- 服务对象的业务和重点决策过程；
- 服务对象的业务连续性。

2．抑制方法认可

如果应急服务由外部组织提供，则外部应急服务提供者应迅速将所确定的抑制方法和相应的措施告知系统运营者，得到系统运营者的认可。

抑制措施可能对系统产生较大影响，应急服务提供者应与系统运营者充分沟通，告知可能存在的风险，制定应变和回退措施，并与其达成协议。

3．抑制实施

应急技术人员应严格按照已确定的技术方案实施抑制，不得随意更改抑制措施和范围，如有必要更改，须还应获得授权。

抑制措施应包含但不限于以下几个方面：

- 监视系统和网络活动；
- 提高系统或网络行为的监控级别；
- 修改防火墙和路由器的过滤规则；
- 尽可能停用系统服务；
- 停止文件共享；
- 改变口令；
- 停用或删除被攻破的登录账号；
- 将被攻陷系统从网络断开；
- 暂时关掉被攻陷系统；
- 设置陷阱，如蜜罐系统；
- 反击攻击者的系统等。

应急技术人员使用的工具应当十分可信，不得使用受害系统已有的不可信文件。

9.3.4 根除阶段

根除阶段的目标是在事件被抑制之后，通过对有关恶意代码或行为的分析结果，找出导致网络安全事件发生的根源，并予以彻底消除。对于单机上的事件，可以根据各种操作系统平台的具体检查和根除程序进行操作即可。但是大规模爆发的带有蠕虫性质的恶意程序，要根除各个主机上的恶意代码，则需投入更大的人力物力。

该阶段的控制点包括三个：根除方法确定、根除方法认可、根除实施。

1．根除方法确定

应急技术人员应检查所有受影响的系统，在准确判断信息安全事件原因的基础上，提出根除的方案建议。

由于入侵者一般都会安装后门或使用其它的方法以便于在将来有来有机会侵入该被攻陷的系统，因此在确定根除方法时，需要了解攻击者是如何入侵的，以及与这种入侵方法相同和类似的各种方法。

2．根除方法认可

与前一阶段类似，应急服务提供者应明确告知系统运营者所采取的根除措施可能带来的风险，制定应变和回退措施，并获得系统运营者的书面授权。

3．根除实施

应急技术人员应使用可信的工具进行安全事件的根除处理，不得使用受害系统已有的不可信文件。

根除措施应包含但不限于以下几个方面：

- 改变全部可能受到攻击的系统的口令；
- 去除所有的入侵通路和入侵者做的修改；
- 修补系统和网络漏洞；
- 增强防护功能，复查所有防护措施(如防火墙)的配置，并依照不同的入侵行为进行调整，对未受防护或者防护不够的网络增加新的防护措施；
- 提高检测功能，对诸如入侵检测系统和其它的入侵报告工具等检测功能及时更新，以保证将来对类似的入侵进行检测；
- 重新安装系统，并对系统进行调整，包括打补丁、修改系统错误，以保证系统不会出现其它的漏洞。

9.3.5 恢复阶段

恢复阶段的目标是将信息安全事件所涉及的系统还原到正常状态。恢复工作应该十分小心，避免出现误操作导致数据的丢失。恢复阶段的行动集中于建立临时业务处理能力、修复原系统损害、在原系统或新设施中恢复运行业务能力等应急措施。

该阶段的控制点包括两个：恢复方法确定和恢复系统。

1．恢复方法确定

应急技术人员应确定一个或多个能从网络安全事件中恢复系统的方法，这些方法应全部告知系统运营者，包括每种方法可能存在的风险。

恢复方案涉及到以下方面：

- 如何获得访问受损设施和/或地理区域的授权；
- 如何通知相关系统的内部和外部业务伙伴；
- 如何获得所需的办公用品和工作空间；
- 如何获得安装所需的硬件部件；
- 如何获得装载备份介质；
- 如何恢复关键操作系统和应用软件；
- 如何恢复系统数据；
- 如何成功运行备用设备。

2．恢复系统

在开始恢复系统时，系统运营者应按照系统的初始化安全策略恢复系统。由于需要恢复的系统可能很多，应根据系统中各子系统的重要性，确定系统恢复的顺序。

系统恢复过程包含但不限于：

- 利用正确的备份恢复用户数据和配置信息，要求使用最近的可靠的备份来进行恢

复；

- 开启系统和应用服务，将由于受到入侵或者怀疑存在漏洞而关闭的服务程序经修改后重新开放；
- 将恢复后的系统连接到网络。

对于不能彻底恢复配置和清除系统上的恶意文件，或不能肯定系统经过根除处理后是否已恢复正常时，应选择彻底重建系统。

一般情况下，如果信息安全事件是由于系统自身原因造成的，则还应在恢复的同时对系统进行全面的安全加固。

9.3.6 总结阶段

总结阶段的目标是回顾信息安全事件处理的全过程，整理与事件相关的各种信息，并尽可能地把所有情况记录到文档中。这些记录的内容，不仅对有关部门的其它处理工作具有重要意义，而且对将来应急工作的开展也是非常重要的积累。

该阶段的控制点包括两个：总结、报告。

1．总结

应急技术人员应及时检查信息安全事件处理记录是否齐全，是否具备可追溯性，并对事件处理过程进行全面总结和分析。

应急响应总结的具体工作包括：

- 事件发生原因分析；
- 事件现象总结；
- 系统的损害程度评估；
- 事件损失估计；
- 应急处置记录进行总结。

2．报告

这是应急处理工作的最后一项。应急技术人员应制定完备的信息安全事件处理报告，并在报告中提出明确的信息安全方面的建议和意见。

9.4 信息系统灾难恢复

本节以国家标准 GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》的内容为基础，介绍了信息系统灾难恢复的基础知识，包括灾难恢复能力的等级划分、灾难恢复需求的确定、灾难恢复策略的制定、灾难恢复策略的实现以及灾难恢复预案的制定、落实和管理。

9.4.1 概述

1．灾难恢复的工作范围

信息系统的灾难恢复工作，包括灾难恢复规划和灾难备份中心的日常运行、关键业务功能在灾难备份中心的恢复和重续运行，以及主系统的灾后重建和回退工作，还涉及突发事件发生后的应急响应。

其中，灾难恢复规划是一个周而复始、持续改进的过程，包含以下几个阶段：

- 灾难恢复需求的确定；
- 灾难恢复策略的制定；
- 灾难恢复策略的实现；
- 灾难恢复预案的制定、落实和管理。

2．灾难恢复的组织机构

1）组织机构的设立

信息系统的运营者应结合其日常组织机构建立灾难恢复的组织机构，并明确其职责。其中一些人可负责两种或多种职责，一些职位可由多人担任（灾难恢复预案中应明确其替代顺序）。

灾难恢复的组织机构由管理、业务、技术和行政后勤等人员组成，一般可设为灾难恢复领导小组、灾难恢复规划实施组和灾难恢复日常运行组。

系统运营单位可聘请具有相应资质的外部专家协助灾难恢复实施工作，也可委托具有相应资质的外部机构承担实施组以及日常运行组的部分或全部工作。

2）组织机构的职责

灾难恢复领导小组是信息系统灾难恢复工作的组织领导机构，组长应由组织最高管理层成员担任。领导小组的职责是领导和决策信息系统灾难恢复的重大事宜，主要如下：

- 审核并批准经费预算；
- 审核并批准灾难恢复策略；
- 审核并批准灾难恢复预案；
- 批准灾难恢复预案的执行。

灾难恢复规划实施组的主要职责是负责：

- 灾难恢复的需求分析；
- 提出灾难恢复策略和等级；
- 灾难恢复策略的实现；
- 制定灾难恢复预案；
- 组织灾难恢复预案的测试和演练。

灾难恢复日常运行组的主要职责是负责：

- 协助灾难恢复系统实施；
- 灾难备份中心日常管理；
- 灾难备份系统的运行和维护；
- 灾难恢复的专业技术支持；
- 参与和协助灾难恢复预案的教育、培训和演练；
- 维护和管理灾难恢复预案；
- 突发事件发生时的损失控制和损害评估；
- 灾难发生后信息系统和业务功能的恢复；
- 灾难发生后的外部协作。

3．灾难恢复规划的管理

信息系统运营者应评估灾难恢复规划过程的风险、筹备所需资源、确定详细任务及时间表、监督和管理规划活动、跟踪和报告任务进展以及进行问题管理和变更管理。

4．灾难恢复的外部协作

信息系统运营者应与相关管理部门、设备及服务提供商、电信、电力和新闻媒体等保持联络和协作，以确保在灾难发生时能及时通报准确情况和获得适当支持。

5．灾难恢复的审计和备案

灾难恢复的等级评定、灾难恢复预案的制定，应按有关规定进行审计和备案。

9.4.2 灾难恢复能力的等级划分

我国国家标准 GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》将灾难恢复能力划分为 6 个级别，由低到高逐级增强。

1．第 1 级：基本支持

第 1 级灾难恢复应具有的技术和管理支持如表 9-1 所示。

表 9-1　第 1 级——基本支持

要素	要求
数据备份系统	a) 完全数据备份至少每周一次； b) 备份介质场外存放。
备用数据处理系统	—
备用网络系统	—
备用基础设施	有符合介质存放条件的场地。
专业技术支持能力	—
运行维护管理能力	a) 有介质存取、验证和转储管理制度； b) 按介质特性对备份数据进行定期的有效性验证。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案
注：“—”表示不作要求	

2．第 2 级：备用场地支持

第 2 级灾难恢复应具有的技术和管理支持如表 9-2 所示。

表 9-2　第 2 级——备用场地支持

要素	要求
数据备份系统	a) 完全数据备份至少每周一次； b) 备份介质场外存放。
备用数据处理系统	灾难发生后能在预定时间内调配所需的数据处理设备到备用场地。
备用网络系统	灾难发生后能在预定时间内调配所需的通信线路和网络设备到备用场地。
备用基础设施	a) 有符合介质存放条件的场地； b) 有满足信息系统和关键业务功能恢复运作要求的场地。
专业技术支持能力	—
运行维护管理能力	a) 有介质存取、验证和转储管理制度； b) 按介质特性对备份数据进行定期的有效性验证； c) 有备用站点管理制度； d) 与相关厂商有符合灾难恢复时间要求的紧急供货协议； e) 与相关运营商有符合灾难恢复时间要求的备用通信线路协议。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。
注：“—”表示不作要求	

3．第 3 级：电子传输和部分设备支持

第 3 级灾难恢复应具有的技术和管理支持如表 9-3 所示。

表 9-3　第 3 级——电子传输和部分设备支持

要素	要求
数据备份系统	a) 完全数据备份至少每天一次； b) 备份介质场外存放； c) 每天多次利用通信网络将关键数据定时批量传送至备用场地。
备用数据处理系统	配备灾难恢复所需的部分数据处理设备。
备用网络系统	配备部分通信线路和相应的网络设备。
备用基础设施	a) 有符合介质存放条件的场地； b) 有满足信息系统和关键业务功能恢复运作要求的场地。
专业技术支持能力	在灾难备份中心有专职的计算机机房运行管理人员。
运行维护管理能力	a) 按介质特性对备份数据进行定期的有效性验证； b) 有介质存取、验证和转储管理制度； c) 有备用计算机机房管理制度； d) 有备用数据处理设备硬件维护管理制度； e) 有电子传输数据备份系统运行管理制度。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

4．第 4 级：电子传输及完整设备支持

第 4 级灾难恢复应具有的技术和管理支持如表 9-4 所示。

表 9-4　第 4 级——电子传输及完整设备支持

要素	要求
数据备份系统	a) 完全数据备份至少每天一次； b) 备份介质场外存放； c) 每天多次利用通信网络将关键数据定时批量传送至备用场地。
备用数据处理系统	配备灾难恢复所需的全部数据处理设备，并处于就绪状态或运行状态。

备用网络系统	a) 配备灾难恢复所需的通信线路； b) 配备灾难恢复所需的网络设备，并处于就绪状态。
备用基础设施	a) 有符合介质存放条件的场地； b) 有符合备用数据处理系统和备用网络设备运行要求的场地； c) 有满足关键业务功能恢复运作要求的场地； d) 以上场地应保持7x24小时运作。
专业技术支持能力	在灾难备份中心有： a) 7x24小时专职计算机机房管理人员； b) 专职数据备份技术支持人员； c) 专职硬件、网络技术支持人员。
运行维护管理能力	a) 有介质存取、验证和转储管理制度； b) 按介质特性对备份数据进行定期的有效性验证； c) 有备用计算机机房运行管理制度； d) 有硬件和网络运行管理制度； e) 有电子传输数据备份系统运行管理制度。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

5．第 5 级：实时数据传输及完整设备支持

第五级灾难恢复应具有的技术和管理支持如表 9-5 所示。

表 9-5　第 5 级——实时数据传输及完整设备支持

要素	要求
数据备份系统	a) 完全数据备份至少每天一次； b) 备份介质场外存放； c) 采用远程数据复制技术，并利用通信网络将关键数据实时复制到备用场地。
备用数据处理系统	配备灾难恢复所需的全部数据处理设备，并处于就绪或运行状态。
备用网络系统	a) 配备灾难恢复所需的通信线路； b) 配备灾难恢复所需的网络设备，并处于就绪状态； c) 具备通信网络自动或集中切换能力。
备用基础设施	a) 有符合介质存放条件的场地； b) 有符合备用数据处理系统和备用网络设备运行要求的场地； c) 有满足关键业务功能恢复运作要求的场地； d) 以上场地应保持7x24小时运作。
专业技术支持能力	在灾难备份中心7x24小时有专职的： a) 计算机机房管理人员； b) 数据备份技术支持人员； c) 硬件、网络技术支持人员。
运行维护管理能力	a) 有介质存取、验证和转储管理制度； b) 按介质特性对备份数据进行定期的有效性验证； c) 有备用计算机机房运行管理制度； d) 有硬件和网络运行管理制度； e) 有实时数据备份系统运行管理制度。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

6．第 6 级：数据零丢失和远程集群支持

第六级灾难恢复应具有的技术和管理支持如表 9-6 所示。

表 9-6　第 6 级——数据零丢失和远程集群支持

要素	要求
数据备份系统	a) 完全数据备份至少每天一次； b) 备份介质场外存放； c) 远程实时备份，实现数据零丢失。
备用数据处理系统	a) 备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容； b) 应用软件是“集群的”，可实时无缝切换； c) 具备远程集群系统的实时监控和自动切换能力。
备用网络系统	a) 配备与主系统相同等级的通信线路和网络设备； b) 备用网络处于运行状态； c) 最终用户可通过网络同时接入主、备中心。
备用基础设施	a) 有符合介质存放条件的场地； b) 有符合备用数据处理系统和备用网络设备运行要求的场地； c) 有满足关键业务功能恢复运作要求的场地； d) 以上场地应保持7x24小时运作。
专业技术支持能力	在灾难备份中心7x24小时有专职的： a) 计算机机房管理人员； b) 专职数据备份技术支持人员； c) 专职硬件、网络技术支持人员； d) 专职操作系统、数据库和应用软件技术支持人员。

运行维护管理能力	a) 有介质存取、验证和转储管理制度； b) 按介质特性对备份数据进行定期的有效性验证； c) 有备用计算机机房运行管理制度； d) 有硬件和网络运行管理制度； e) 有实时数据备份系统运行管理制度； f) 有操作系统、数据库和应用软件运行管理制度。
灾难恢复预案	有相应的经过完整测试和演练的灾难恢复预案。

9.4.3 灾难恢复需求的确定

1．风险分析

在确定在灾难恢复需求时，应首先进行风险分析，即标识信息系统的资产价值，识别信息系统面临的自然的和人为的威胁，识别信息系统的脆弱性，分析各种威胁发生的可能性，并定量或定性描述可能造成的损失，继而通过技术和管理手段，防范或控制信息系统的风险。要依据防范或控制风险的可行性和残余风险的可接受程度，确定对风险的防范和控制措施。

2．业务影响分析

1）分析业务功能和相关资源配置

对各项业务功能及各项业务功能之间的相关性进行分析，确定支持各种业务功能的相应信息系统资源及其它资源，明确相关信息的保密性、完整性和可用性要求。

2）评估中断影响

采用如下的定量和/或定性的方法，对各种业务功能的中断造成的影响进行评估：

- 定量分析：以量化方法，评估业务功能的中断可能给组织带来的直接经济损失和间接经济损失；
- 定性分析：运用归纳与演绎、分析与综合以及抽象与概括等方法，评估业务功能的中断可能给组织带来的非经济损失，包括组织的声誉、客户的忠诚度、员工的信心、社会和政治影响等。

3．确定灾难恢复目标

根据风险分析和业务影响分析的结果，确定灾难恢复目标，包括：

- 关键业务功能及恢复的优先顺序；
- 灾难恢复时间范围。

9.4.4 灾难恢复策略的制定

1．制定灾难恢复策略的过程

在制定灾难恢复策略时，要着眼于灾难恢复所需的下列资源要素：

- 数据备份系统：一般由数据备份的硬件、软件和数据备份介质（以下简称“介质”）组成，如果是依靠电子传输的数据备份系统，还包括数据备份线路和相应的通信设备；
- 备用数据处理系统：指备用的计算机、外围设备和软件；
- 备用网络系统：最终用户用来访问备用数据处理系统的网络，包含备用网络通信设备和备用数据通信线路；
- 备用基础设施：灾难恢复所需的、支持灾难备份系统运行的建筑、设备和组织，包括介质的场外存放场所、备用的机房及灾难恢复工作辅助设施，以及容许灾难恢复人员连续停留的生活设施；
- 专业技术支持能力：对灾难恢复系统的运转提供支撑和综合保障的能力,以实现灾难恢复系统的预期目标。包括硬件、系统软件和应用软件的问题分析和处理能力、网络系统安全运行管理能力、沟通协调能力等；
- 运行维护管理能力：包括运行环境管理、系统管理、安全管理和变更管理等；
- 灾难恢复预案。

根据灾难恢复目标，按照灾难恢复资源的成本与风险可能造成的损失之间取得平衡的原则（即“成本风险平衡原则”）确定每项关键业务功能的灾难恢复策略，不同的业务功能可采用不同的灾难恢复策略。

灾难恢复策略包括：

- 灾难恢复资源的获取方式；
- 灾难恢复等级，或灾难恢复资源各要素的具体要求。

2．灾难恢复资源的获取方式

1）数据备份系统

数据备份系统可自行建设，也可通过租用其它机构的系统而获取。

2）备用数据处理系统

可选用以下三种方式之一来获取备用数据处理系统：

- 事先与厂商签订紧急供货协议；
- 事先购买所需的数据处理设备并存放在灾难备份中心或安全的设备仓库；
- 利用商业化灾难备份中心或签有互惠协议的机构已有的兼容设备。

3）备用网络系统

备用网络通信设备可通过与获取数据处理系统相同的方式获取；备用数据通信线路可使用自有数据通信线路或租用公用数据通信线路。

4）备用基础设施

可选用以下三种方式获取备用基础设施：

- 由组织所有或运行；
- 多方共建或通过互惠协议获取；
- 租用商业化灾难备份中心的基础设施。

5）专业技术支持能力

可选用以下几种方式获取专业技术支持能力：

- 灾难备份中心设置专职技术支持人员；
- 与厂商签订技术支持或服务合同；
- 由主中心技术支持人员兼任；但对于 RTO 较短的关键业务功能，应考虑到灾难发生时交通和通信的不正常，造成技术支持人员无法提供有效支持的情况。

6）运行维护管理能力

可选用以下对灾难备份中心的运行维护管理模式：

- 自行运行和维护；
- 委托其它机构运行和维护。

7）灾难恢复预案

可选用以下方式，完成灾难恢复预案的制定、落实和管理：

- 由组织独立完成；
- 聘请具有相应资质的外部专家指导完成；
- 委托具有相应资质的外部机构完成。

3．灾难恢复资源的要求

1）数据备份系统

信息系统运营者应根据灾难恢复目标，按照成本风险平衡原则，确定：

- 数据备份的范围；
- 数据备份的时间间隔；
- 数据备份的技术及介质；
- 数据备份线路的速率及相关通信设备的规格和要求。

2）备用数据处理系统

信息系统运营者应根据关键业务功能的灾难恢复对备用数据处理系统的要求和未来发展的需要，按照成本风险平衡原则，确定备用数据处理系统的：

- 数据处理能力；
- 与主系统的兼容性要求；
- 平时处于就绪还是运行状态。

3）备用网络系统

信息系统运营者应根据关键业务功能的灾难恢复对网络容量及切换时间的要求和未来发展的需要，按照成本风险平衡原则，选择备用数据通信的技术和线路带宽，确定网络通信设备的功能和容量，保证灾难恢复时，最终用户能以一定速率连接到备用数据处理系统。

4）备用基础设施

信息系统运营者应根据灾难恢复目标，按照成本风险平衡原则，确定对备用基础设施的要求，包括：

- 与主中心的距离要求；
- 场地和环境（如面积、温度、湿度、防火、电力和工作时间等）要求；
- 运行维护和管理要求。

5）专业技术支持能力

信息系统运营者应根据灾难恢复目标，按照成本风险平衡原则，确定灾难备份中心在软件、硬件和网络等方面的技术支持要求，包括技术支持的组织架构、各类技术支持人员的数量和素质等要求。

6）运行维护管理能力

信息系统运营者应根据灾难恢复目标，按照成本风险平衡原则，确定灾难备份中心运行维护管理要求，包括运行维护管理组织架构、人员的数量量和素质、运行维护管理制度等要求。

7）灾难恢复预案

信息系统运营者应根据需求分析的结果，按照成本风险平衡原则，明确灾难恢复预案的：

- 整体要求；
- 制定过程的要求；
- 教育、培训和演练要求；
- 管理要求。

9.4.5 灾难恢复策略的实现

1．灾难备份系统技术方案的实现

1）技术方案的设计

根据灾难恢复策略制定相应的灾难备份系统技术方案，包含数据备份系统、备用数据处理系统和备用的网络系统。技术方案中所设计的系统，应：

- 获得同主系统相当的安全保护；
- 具有可扩展性；
- 考虑其对主系统可用性和性能的影响。

2）技术方案的验证、确认和系统开发

为确保技术方案满足灾难恢复策略的要求，应由相关部门对技术方案进行确认和验证，并记录和保存验证及确认的结果。

按照确认的灾难备份系统技术方案进行开发，实现所要求的数据备份系统、备用数据处理系统和备用网络系统。

3）系统安装和测试

按照经过确认的技术方案，灾难恢复规划实施组应制定各阶段的系统安装及测试计划，以及支持不同关键业务功能的系统安装及测试计划，并组织最终用户共同进行测试。确认以下各项功能可正确实现：

- 数据备份及数据恢复功能；
- 在限定的时间内，利用备份数据正确恢复系统、应用软件及各类数据，并可正确恢复各项关键业务功能；
- 客户端可与备用数据处理系统通信正常。

2．灾难备份中心的选择和建设

1）选址原则

选择或建设灾难备份中心时，应根据风险分析的结果，避免灾难备份中心与主中心同时遭受同类风险。灾难备份中心包括同城和异地两种类型，以规避不同影响范围的灾难风险。

灾难备份中心应具有数据备份和灾难恢复所需的通信、电力等资源，以及方便灾难恢复人员和设备到达的交通条件。

灾难备份中心应根据统筹规划、资源共享、平战结合的原则，合理地布局。

2）基础设施的要求

新建或选用灾难备份中心的基础设施时：

- 计算机机房应符合有关国家标准的要求；
- 工作辅助设施和生活设施应符合灾难恢复目标的要求。

3．专业技术支持能力的实现

组织应根据灾难恢复策略的要求，获取对灾难备份系统的专业技术支持能力。

灾难备份中心应建立相应的技术支持组织，定期对技术支持人员进行技能培训。

4．运行维护管理能力的实现

为了达到灾难恢复目标，灾难备份中心应建立各种操作和管理制度，用以保证：

- 数据备份的及时性和有效性；
- 备用数据处理系统和备用网络系统处于正常状态，并与主系统的参数保持一致；
- 有效的应急响应、处理能力。

5．灾难恢复预案的实现

灾难恢复的每个等级均应制定相应的灾难恢复预案，并进行落实和管理。

9.4.6　灾难恢复预案的制定、落实和管理

1．灾难恢复预案的制定

1）制定原则

灾难恢复预案的制定原则如下：

- 完整性：灾难恢复预案（以下称预案）应包含灾难恢复的整个过程，以及灾难恢复所需的尽可能全面的数据和资料；
- 易用性：预案应运用易于理解语言和图表，并适合在紧急情况下使用；
- 明确性：预案应采用清晰的结构，对资源进行清楚的描述，工作内容和步骤应具体，每项工作应有明确的责任人；
- 有效性：预案应尽可能满足灾难发生时进行恢复的实际需要，并保持与实际系统和人员组织的同步更新；
- 兼容性：灾难恢复预案应与其它应急预案体系有机结合。

2）制定过程

在灾难恢复预案制定原则的指导下，其制定过程如下：

- 起草：参照附录 B 灾难恢复预案框架，按照风险分析和业务影响分析所确定的灾难恢复内容，根据灾难恢复等级的要求，结合组织其它相关的应急预案，撰写出灾

难恢复预案的初稿；

- 评审：组织应对灾难恢复预案初稿的完整性、易用性、明确性、有效性和兼容性进行严格的评审。评审应有相应的流程保证；
- 测试：应预先制定测试计划，在计划中说明测试的案例。测试应包含基本单元测试、关联测试和整体测试。测试的整个过程应有详细的记录，并形成测试报告；
- 完善：根据评审和测试结果，纠正在初稿评审过程和测试中发现的问题和缺陷，形成预案的审批稿；
- 审核和批准：由灾难恢复领导小组对审批稿进行审核和批准，确定为预案的执行稿。

2．灾难恢复预案的教育、培训和演练

为了使相关人员了解信息系统灾难恢复的目标和流程，熟悉灾难恢复的操作规程，组织应按以下要求，组织灾难恢复预案的教育、培训和演练：

- 在灾难恢复规划的初期就应开始灾难恢复观念的宣传教育工作；
- 预先对培训需求进行评估，包括培训的频次和范围，开发和落实相应的培训/教育课程，保证课程内容与预案的要求相一致，事后保留培训的记录；
- 预先制定演练计划，在计划中说明演练的场景。
- 演练的整个过程应有详细的记录，并形成报告；
- 每年应至少完成一次有最终用户参与的完整演练。

3．灾难恢复预案的管理

1）保存与分发

经过审核和批准的灾难恢复预案，应：

- 由专人负责保存与分发；
- 具有多份拷贝在不同的地点保存；
- 分发给参与灾难恢复工作的所有人员；
- 在每次修订后所有拷贝统一更新，并保留一套，以备查阅；
- 旧版本应按有关规定销毁。

2）维护和变更管理

为了保证灾难恢复预案的有效性，应从以下方面对灾难恢复预案进行严格的维护和变更管理：

- 业务流程的变化、信息系统的变更、人员的变更都应在灾难恢复预案中及时反映；
- 预案在测试、演练和灾难发生后实际执行时，其过程均应有详细的记录，并应对测试、演练和执行的效果进行评估，同时对预案进行相应的修订；
- 灾难恢复预案应定期评审和修订，至少每年一次。

本章小结

本章以现行国家标准为基础，介绍了信息安全应急处理和灾难恢复的知识。本章的目的除了希望读者掌握这些基础知识、增强实践能力外，还希望帮助读者结合前几章的知识构建起以等级保护、风险评估、应急处理、灾难恢复等为主要内容的信息安全防护体系的基本概念。

本章内容主要有：

（1）信息安全事件分类

信息安全事件指由于自然或者人为的原因，对信息系统造成危害，或在信息系统内发生对社会造成负面影响的事件。根据国家标准 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》，信息安全事件可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其它信息安全事件等 7 个基本分类，每个基

本分类分别包括若干个子类。

（2）信息安全事件分级

对信息安全事件的分级参考下列三个要素：信息系统的重要程度、系统损失和社会影响。其中，系统损失划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失；社会影响划分为特别重大的社会影响、重大的社会影响、较大的社会影响和一般的社会影响。根据这些信息安全事件分级参考要素，将信息安全事件划分为四个级别：特别重大事件、重大事件、较大事件和一般事件。

（3）信息安全应急处理关键过程

应急处理关键过程可分为 6 个阶段：准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段和总结阶段。每个阶段各自包括具体的工作内容，总计 17 项。

（4）信息系统灾难恢复

以国家标准 GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》的内容为基础，本章还介绍了信息系统灾难恢复的基础知识，包括灾难恢复能力的等级划分、灾难恢复需求的确定、灾难恢复策略的制定、灾难恢复策略的实现以及灾难恢复预案的制定、落实和管理。

灾难恢复能力共分为 6 级：基本支持级、备用场地支持级、电子传输和部分设备支持级、电子传输及完整设备支持级、实时数据传输及完整设备支持级、数据零丢失和远程集群支持级。在确定在灾难恢复需求时，应首先进行风险分析，在此基础上分析信息安全事件对业务的影响，确定灾难恢复目标。在制定灾难恢复策略时，要着眼于灾难恢复所需的资源要素。策略中要明确灾难恢复资源的获取方式以及所需的灾难恢复等级，或灾难恢复资源要素的具体要求。在实施灾难恢复策略时，一方面要实现备份系统技术方案，另一方面要选择好灾难备份中心，此外还应获得专业技术支持能力和运行维护管理能力，并最终确立灾难恢复预案。对灾难恢复预案，要进行严格的管理和落实，并积极进行演练。

习题

1．信息安全事件如何分类？
2．信息安全事件如何分级？需要考虑那些要素？
3．信息安全应急处理关键过程包括几个阶段？各阶段的主要内容是什么？
4．信息安全应急处理与灾难恢复的区别和联系是什么？
5．灾难恢复能力的等级是怎样划分的？
6．如何确定灾难恢复需求？
7．灾难恢复策略包括哪些内容？如何制定灾难恢复策略？
8．如何制定灾难恢复预案？如何对灾难恢复预案进行管理？

第 10 章　信息安全法规和标准

本章要点

- 我国《立法法》规定的法律层次
- 我国信息安全立法存在的问题
- 标准的分类
- 我国信息安全标准化工作概况
- 主要的国外信息安全标准化组织
- 信息安全评估国际标准的发展

10.1　法律基础

在介绍信息安全法律法规之前，本节首先介绍了一些法律方面的基础知识。法是由一定社会物质生活条件所决定的，由国家制定和认可的，并由国家强制力保证实施的具有普遍约束力的行为规范的总和。法的目的在于维护、巩固和发展一定的社会关系和社会次序。德国学者耶林将法律目的，比喻为在茫茫大海上指引航船方向的“导引之星”（北极星）。因此，学习、理解和运用法律，需要了解法的意义和作用，掌握法律体系的构成。

10.1.1　法的意义与作用

1．意义

具体说来，法律的意义有如下几点：

（1）法律的秩序意义。法律在构建社会秩序中起着主要作用，法律的形成保证着人类的生存，保证着社会的发展。在现代社会，国家意志在秩序形成中具有重大作用，这取决于人对理性能力的确信。

（2）法律的自由意义。法律提供给个人选择的机会，法律明确行为模式，让行为人选择有利于自己的模式。另外，法律将个人自由赋予法律的形式，成为法律权利，使自由得到国家强制力的保护。最后，法律通过划定自由的界限，为普遍自由的实现提供前提。法律即使限制自由也是为了每个人更好地实现自由。

（3）法律的正义意义。正义是法律的理想或价值目标，法律通过分配权利义务，惩罚违法犯罪以保障正义，补偿受害者以恢复正义。

（4）法律的效率意义。在当代，法律对生活的渗透无所不在，这使得法律的效率意义更加重要。在提倡兼顾平等与效率的同时，法律最大限度地保障了效率的实现。

（5）法律的利益意义。法律确认利益，通过平衡冲突进行社会控制，解决社会纠纷，平息社会矛盾，恢复社会常态，促进社会发展

2．作用

唯物史观认为，法的作用体现在法与社会的交互影响中，在社会发展的过程中，法作为上层建筑的组成部分，其产生、存在与发展变化都是由社会的生产方式决定的。法在由社会所决定的同时，也具有相对的独立性。法的作用直接表现为国家权力的行使。法律的作用与国家的地位和作用互为表里。法的作用本质上是社会自身力量的体现。法能否对社会发生作用，法对社会作用的程度，法对社会所发生作用的效果，不是法律自身能够决定的。

法的作用可以分为规范作用与社会作用。

法的规范作用可分为：

（1）指引作用，指法对本人的行为具有引导作用。对人的行为的指引有两种形式：①个别性指引，即通过一个具体的指示形成对具体的人的具体情况的指引；②规范性指引，是通过一般的规则对同类的人或行为的指引。从立法技术上看，法律对人的行为的指引通常采用两种方式：①确定的指引，即通过设置法律义务，要求人们作出或抑制一定行为，使社会成员明确自己必须从事或不得从事的行为界限。②不确定的指引，又称选择的指引，是指通过宣告法律权利，给人们一定的选择范围。

（2）评价作用：法律作为一种行为标准，具有判断、衡量他人行为合法与否的评判作用。

（3）教育作用：指通过法的实施使法律对一般人的行为产生影响。这种作用又具体表现为示警作用和示范作用。

（4）预测作用：凭借法律的存在，可以预先估计到人们相互之间会如何行为。

（5）强制作用：指法可以通过制裁违法犯罪行为来强制人们遵守法律。

法的社会作用主要体现在社会经济生活、政治生活、思想文化三个领域，具有政治职能（阶级统治的职能）和社会职能（执行社会公共事务的职能）。法律在执行社会公共事务上的作用具体表现在这样一些方面：①维护人类社会的基本生活条件；②维护生产和交换条件；③促进公共设施建设，组织社会化大生产；④确认和执行技术规范；⑤促进教育、科学和文化事业的发展。

尽管法在社会生活中具有重要作用，但是，法律不是万能的。法律是以社会为基础的，因此，法律不可能超出社会发展需要“创造”社会。法律作为社会规范之一，必然受到其它社会规范以及社会条件和环境的制约。法律还有着自身条件的制约，如语言表达力的局限。因此，认识法律的作用必须注意“两点论”：对法律的作用既不能夸大，也不能忽视；既认识到法律不是无用的，又要认识到法律不是万能的；既要反对“法律无用论”，又要防止“法律万能论”。

10.1.2 我国《立法法》规定的法律层次

2000 年 3 月由九届全国人大第三次会议审议通过，并于 2000 年 7 月 1 日起正式实施的《中华人民共和国立法法》，是我国规范立法活动的一部宪法性法律。一切立法活动都必须以《中华人民共和国立法法》为依据，遵循立法法的有关规定。在此之前，我国规范立法活动的规范主要是宪法、有关法律和行政性法规。由于这些规范不统一、不完善和过分原则化，不仅造成了操作上的困难，而且导致了大量无权立法、越权立法、借法扩权、立法侵权等立法异常现象。《中华人民共和国立法法》确立了法律优先原则，即在多层次立法的情况下，除宪法外，由国家立法机关所制定的法律处于最高位阶、最优地位，其它任何形式的法规都必须与之保持一致，不得抵触。我国是统一的、单一制的国家，各地方经济、社会发展又很不平衡。与这一国情相适应，在最高国家权力机关集中行使立法权的前提下，为了使我们的法律既能通行全国，又能适应各地方千差万别的不同情况的需要，在实践中能行得通，宪法和立法法根据宪法确定的“在中央的统一领导下，充分发挥地方的主动性、积极性”的原则，确立了我国的统一而又分层次的立法体制：

（1）全国人大及其常委会行使国家立法权。全国人大制定和修改刑事、民事、国家机构的和其它的基本法律。全国人大常委会制定和修改除应当由全国 人大制定的法律以外的其它法律；在全国人大闭会期间，对全国人大制定的法律进行部分补充和修改，但不得同该法律的基本原则相抵触。

（2）国务院即中央人民政府根据宪法和法律，制定行政法规。

（3）省、自治区、直辖市的人大及其常委会根据本行政区域的具体情况和实际需要，在不同宪法、法律、行政法规相抵触的前提下，可以制定地方性法规；较大的市（包括省、

自治区人民政府所在地的市、经济特区所在地的市和经国务院批准的较大的市）的人大及其常委会根据本市的具体情况和实际需要，在不同宪法，法律、行政法规和本省、自治区的地方性法规相抵触的前提下，可以制定地方性法规，报省、自治区的人大常委会批准后施行。

（4）经济特区所在地的省、市的人大及其常委会根据全国人大的授权决定，还可以制定法规，在经济特区范围内实施。

（5）自治区、自治州、自治县的人大还有权依照当地民族的政治、经济和文化的特点，制定自治条例和单行条例，对法律、行政法规的规定作出变通规定。自治区的自治条例和单行条例报全国人大常委会批准后生效，自治州、自治县的自治条例和单行条例报省、自治区、直辖市的人大常委会批准后生效。

（6）国务院各部、各委员会、中国人民银行、审计署和具有行政管理职能的直属机构，可以根据法律和国务院的行政法规、决定、命令，在本部门的权限范围内，制定规章。省、自治区、直辖市和较大的市的人民政府，可以根据法律、行政法规和本省、自治区、直辖市的地方性法规，制定规章。

宪法和有关法律的这些规定表明，我国的立法体制既是统一的，又是分层次的，是由国家立法权和行政法规制定权、地方性法规制定权、自治条例和单行条例制定权以及授权立法权所构成的，同时下位阶的法的规范不能和上位阶的法的规范相抵触。宪法具有最高的法律效力，一切法律、法规都不得同宪法相抵触。法律的效力高于行政法规，行政法规不得同法律相抵触。法律、行政法规的效力高于地方性法规和规章，地方性法规和规章不得同法律、行政法规相抵触。地方性法规的效力高于地方政府规章，地方政府规章不得同地方性法规相抵触。这样一个立法体制，说明地方立法，从性质上讲，应当是对中央立法（制定法律、行政法规）的补充，行政法规也是对国家法律的补充，都是国家法律体系的组成部分。

这样一个立法体制，也可以说主要体现了以下两个精神：一是在中央与地方关系上，既坚持中央必要的集中统一，又注意充分发挥地方的主动性、积极性。二是在权力机关与行政机关的关系上，既坚持了人民代表大会制度，保证立法权掌握在由人民选举产生的、更有利于直接反映群众意愿和要求的国家权力机关手里，以保证立法的民主性；同时，又注意提高国家的管理效率，保证国家行政机关有足够的权力对社会进行有效管理。

10.2 我国信息安全法律体系

我国目前的信息化立法，尤其是信息安全立法，尚处于起步阶段，我国政府和法律界都清醒地意识到这一问题的重要性，正在积极推进这一方面的工作。我国政府现有的信息安全法律体系可以分为两个层次。一是法律层次，从国家宪法和其它部门法的高度对个人、法人和其它组织的涉及国家安全的信息活动的权利和义务进行规范，例如 1997 年新《刑法》首次界定了计算机犯罪。二是行政法规和部门规章层次，直接约束计算机安全和互联网安全。此外，我国很多地方也出台了直接针对信息安全的地方性法规和地方政府规章，丰富了我国信息安全法律体系的内容。

10.2.1 主要信息安全法律

这一层面是指由全国人民代表大会及其常务委员会通过的法律规范，

我国法律中涉及到信息安全的有：

（1）中华人民共和国宪法（第四十条）

（2）中华人民共和国保守国家秘密法

（3）中华人民共和国国家安全法（第十条、十一条等）

（4）中华人民共和国人民警察法（第六条、十六条等）

（5）中华人民共和国刑法（第二百八十五条、二百八十六条、二百八十七条等）

（6）全国人民代表大会常务委员会关于维护互联网安全的决定

（7）中华人民共和国电子签名法

（8）中华人民共和国治安管理处罚法（第二十九条、四十二条等）

10.2.2 主要信息安全行政法规

我国行政法规中涉及到信息安全的有：

（1）中华人民共和国计算机信息系统安全保护条例

（2）中华人民共和国计算机信息网络国际联网管理暂行规定

（3）商用密码管理条例

（4）中华人民共和国电信条例

（5）互联网信息服务管理办法

（6）互联网上网服务营业场所管理条例

（7）信息网络传播权保护条例

10.2.3 主要信息安全部门规章

我国已发布涉及信息安全的部门规章的政府部门有公安部、原信息产业部、国务院新闻办、国家保密局、文化部、原国家科委、新闻出版总署、国家版权局、国家广播电影电视总局、铁道部、国家药监局、中国银监会等部门。这些部门规章中，有相当一部分涉及到互联网的管理问题和信息安全问题。

这些部门规章包括：

（1）计算机信息系统安全专用产品检测和销售许可证管理办法（公安部令第 32 号）

（2）计算机信息网络国际联网安全保护管理办法（公安部令第 33 号）

（3）计算机病毒防治管理办法（公安部令第 51 号）

（4）互联网安全保护技术措施规定（公安部令第 82 号）

（5）互联网电子公告服务管理规定（信息产业部令第 3 号）

（6）电信业务经营许可证管理办法（信息产业部令第 19 号）

（7）中国互联网络域名管理办法（信息产业部令第 30 号）

（9）非经营性互联网信息服务备案管理办法（信息产业部令第 33 号）

（10）互联网 IP 地址备案管理办法（信息产业部令第 34 号）

（11）电子认证服务管理办法（信息产业部令第 35 号）

（12）互联网电子邮件服务管理办法（信息产业部令第 38 号）

（13）互联网新闻信息服务管理规定（国务院新闻办公室、信息产业部令第 37 号）

（14）中华人民共和国保守国家秘密法实施办法（国家保密局令第 1 号）

（15）科学技术保密规定（国家科委、国家保密局令第 20 号）

（16）互联网文化管理暂行规定（文化部令第 27 号）

（17）电子出版物管理规定（新闻出版总署令第 11 号）

（18）互联网出版管理暂行规定（新闻出版总署、信息产业部令第 17 号）

（19）互联网著作权行政保护办法（国家版权局、信息产业部令第 5 号）

（20）有线广播电视传输覆盖网安全管理办法（国家广播电影电视总局令第 13 号）

（21）互联网等信息网络传播视听节目管理办法（国家广播电影电视总局令第 39 号）

（22）互联网药品信息服务管理暂行规定（国家药品监督管理局令第 26 号）

（23）电子银行业务管理办法（中国银行业监督管理委员会令 2006 年第 5 号）

10.2.4 地方性法规和地方政府规章

我国一些地方人民代表大会和人民政府近年来也发布了一些地方性法规和地方政府规章。包括各省、自治区、直辖市人民代表大会及其常务委员会根据本行政区域的具体情况和实际需要，在不与宪法、法律、行政法规相抵触的前提下制定的地方性法规；各省、自治区、直辖市人民政府根据法律、行政法规和本省、自治区、直辖市的地方性法规制定的地方政府

规章。

其中，涉及信息安全的地方性法规主要包括：

（1）辽宁省计算机信息系统安全管理条例

（2）湖南省信息化条例

（3）重庆市计算机信息系统安全保护条例

（4）北京市信息化促进条例

（5）天津市信息化促进条例

（6）山东省信息化促进条例

（7）广东省计算机信息系统安全保护条例

（8）山西省计算机信息系统安全保护条例

涉及信息安全的地方政府规章主要包括：

（1）福建省计算机信息系统安全管理办法

（2）四川省计算机信息系统安全保护管理办法

（3）山西省计算机安全管理规定

（4）黑龙江省计算机信息系统安全管理规定

（5）山东省计算机信息系统安全管理办法

（6）深圳经济特区计算机信息系统公共安全管理规定

（7）安徽省计算机信息系统安全保护办法

（8）辽宁省计算机信息保密管理规定

（9）河南省计算机信息系统安全保护暂行办法

（10）天津市公共计算机信息网络安全保护规定

（11）江苏省计算机信息系统安全保护管理办法

（12）广东省计算机信息系统安全保护管理规定

（13）广东省计算机信息系统安全保护管理规定实施细则（试行）

（14）云南省网络与信息系统安全监察管理规定

（15）江西省计算机信息系统安全保护办法

（16）杭州市计算机信息系统安全保护管理办法

（17）北京市公共服务网络与信息系统安全管理规定

（18）浙江省信息安全等级保护管理办法

10.2.5 我国信息安全立法存在的问题

从以上情况看，我国的信息安全立法工作揖经具有了一定的基础，初步形成了信息安全法律体系，为我国信息安全保障工作创造了良好的法律环境，为依法规范和保护我国信息化建设健康有序发展提供了有利的法律依据。但是，我国的信息立法也存在诸多问题，主要表现在：

（1）结构不合理。大多为行政规章、规范和制度，没有一部针对国家信息安全的专门法律。虽然《中华人民共和国电子签名法》是我国第一部信息化法律，也是第一部信息安全法律，特其只规范了信息安全领域内的一个非常具体的问题，我国仍然缺少综合性的信息安全法律。

（2）已有的规章制度出自多个部门，相互之间缺乏统筹规划，法规的协调性和相通性不够，甚至同一行为有多个行政处罚主体、不同部门发布的规章有明显的相互矛盾之处。

（3）有些法规制度的制订实施，过于原则或笼统，没有来得及做深入细致的调查研究、充分论证和广泛征求意见，针对性和操作性不够强。

（4）有些法规制度明显滞后。例如，现有法律对新型网络犯罪缺乏应对，纵览现行全部有关信息安全的法律规范，竟没有一条能适用诸如“安置逻辑炸弹”、“开办黑客培训学校”

等行为。这表明现行信息安全法律规范滞后于信息网络技术的发展，不能适应信息网络犯罪手段不断翻新、技术对抗日趋明显的严峻形势。此外，目前的信息安全法律体系对网络犯罪处罚过轻，威慑力不够。

（5）公民个人权益缺乏法律保护，较为突出的是《个人信息保护法》迟迟不能制定，全社会反映强烈，两会代表、委员多次提交于此相关的建议和提案。

（6）刑事程序立法亟需完善。《刑事诉讼法》中对信息网络犯罪案件的调查取证程序没有做出明确的规定。《公安机关办理刑事案件程序规定》只规定了扣押书证、物证的范围包括电子邮件，而电子邮件只是信息网络的功能之一，上述规定无论是调查范围，还是取证程序上都无法涵盖有关信息网络犯罪案件的调查取证问题。因此，亟待对有关信息网络犯罪案件的调查取证程序做出明确的法律规定。

10.2.6 我国信息安全立法工作进展

我国在 1997 年全面修订《刑法》时，明确规定了计算机犯罪的罪名，即：第 285 条的非法侵入计算机信息系统罪，第 286 条的破坏计算机信息系统罪和第 287 条的利用计算机进行传统犯罪。但是，《刑法》第 285 条“非法侵入计算机信息系统罪”规定的犯罪对象过于狭窄，只限于“国家事务、国防建设、尖端科学技术领域”，而第 286 条“破坏计算机信息系统罪”只有在“造成计算机信息系统不能正常运行”等严重后果的情况下，才对犯罪分子予以追究，这导致人民法院对很多侵犯信息安全的案件束手无策。

为了改变《刑法》严重滞后的局面，全国人大常委会在 2009 年 2 月发布《刑法修正案（七）》，将入侵国家事务、国防建设、尖端科学技术领域之外的信息系统的行为纳入了打击范围。此外，第 285 条还规定，提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，同样按照“非法侵入计算机信息系统罪”的规定处罚。《刑法》此次修改是我国信息安全立法工作中取得的重要成绩，对打击网络犯罪具有十分重要的意义。

我国在 1989 年 5 月 1 日起施行了《中华人民共和国保守国家秘密法》，对于保守国家秘密、维护国家安全和利益，发挥了重要作用。然而，随着我国经济社会的快速发展，特别是信息化的发展和电子政务的建设与应用，保密工作中出现了一些新情况和新问题，亟待通过修改法律来解决。例如，国家秘密存在的形态和运行的方式发生了变化，国家秘密载体由纸介质形式为主发展到声、光、电、磁等多种形式，同时保密工作的对象、领域和环境也发生了深刻变化，一些经济和社会组织进入涉密领域。现行保密法关于保密法律责任的规定已经不能适应新形势下保密工作的需要。现代通信和计算机网络条件下存储、处理和传输国家秘密的制度以及涉密机关、单位和涉密人员的保密管理制度和法律责任都需要补充完善。为此，保密法的修订已经进入立法程序，并经过了十一届全国人大常委会第九次会议的首次审议，目前正在进一步征求社会意见。新的保密法草案针对当前涉密信息系统频繁泄密的严峻形势，特别增加了保密措施，强化了法律责任要求，这标志着我国保密工作将进入新的发展阶段。

为了建立和完善信息安全法律制度，确立信息安全的基础法律框架，目前《信息安全条例》的起草工作正在抓紧进行，我国信息安全立法工作中存在的很多问题，特别是缺少综合性的信息安全专门法的局面将很快得以改善。

10.3 标准基础

标准是对重复性事物和概念所做的统一规定，它以科学、技术和实践经验的综合成果为基础，经有关方面协商一致，由主管机构批准，以特定形式发布，作为共同遵守的准则和依据。本小节介绍了标准的基础知识，包括基本概念、标准的意义与作用、标准的层次与类别。

10.3.1 基本概念

下面首先介绍与标准相关的一些重要概念，主要包括：

标准化是指在经济、技术、科学及管理等社会实践中，对重复性事物和概念通过制定、发布和实施标准，达到统一，以获得最佳秩序和社会效益的活动。

强制性标准是国家通过法律的形式明确要求对于一些标准所规定的技术内容和要求必须执行，不允许以任何理由或方式加以违反、变更，这样的标准称之为强制性标准，包括强制性的国家标准、行业标准和地方标准。对违反强制性标准的，国家将依法追究当事人法律责任。

推荐性标准是指国家鼓励自愿采用的具有指导作用而又不宜强制执行的标准，即标准所规定的技术内容和要求具有普遍的指导作用，允许使用单位结合自己的实际情况，灵活加以选用。国际标准是指国际标准化组织 ISO 和国际电工委员会 IEC 所制定的标准，以及国际标准化组织已列入《国际标准题内关键词索引》中的 27 个国际组织制定的标准和公认具有国际先进水平的其它国际组织制定的某些标准。

国外先进标准是指国际上有影响的区域标准，世界主要经济发达国家制定的国家标准和其他国家某些具有世界先进水平的国家标准，国际上通行的团体标准以及先进的企业标准。

采用国际标准包括采用国外先进标准，是指把国际标准和国外先进标准的内容，通过分析研究，不同程度地纳入我国的各级标准中，并贯彻实施以取得最佳效果的活动。

制定标准是指标准制定部门对需要制定标准的项目，编制计划，组织草拟、审批、编号、发布的活动。它是标准化工作任务之一，也是标准化活动的起点。

标准备案是指一项标准在其发布后，负责制定标准的部门或单位，将该项标准文本及有关材料，送标准化行政主管部门及有关行政主管部门存案以备查考的活动。 标准复审是指对使用一定时期后的标准，由其制定部门根据我国科学技术的发展和经济建设的需要，对标准的技术内容和指标水平所进行的重新审核，以确认标准有 效性的活动。

标准的实施是指有组织、有计划、有措施地贯彻执行标准的活动，是标准制定部门、使用部门或企业将标准规定的内容贯彻到生产、流通、使用等领域中去的过程。它是标准化工作的任务之一，也是标准化工作的目的。

标准实施监督是国家行政机关对标准贯彻执行情况进行督促、检查、处理的活动。它是政府标准化行政主管部门和其他有关行政主管部门领导和管理标准化活动的重要手段，也是标准化工作任务之一，其目的是促进标准的贯彻，监督标准贯彻执行的效果，考核标准的先进性和合理性，通过标准实施的监督，随时发现标准中存在的问题，为进一步修订标准提供依据。标准体制是与实现某一特定的标准化目的有关的标准，按其内在联系，根据一些要求所形成的科学的有机整体。它是有关标准分级和标准属性的总体，反映了标准之间相互连接、相互依存、相互制约的内在联系。

等同采用国际标准是采用国际标准的基本方法之一。它是指我国标准在技术内容与文本结构均与国际标准完全相同，或者我国标准在技术内容上与国际标准相同，但可以包含小的编辑性修改，其缩写字母代号为 IDT。等同采用国际标准适用“反之亦然原则”。

修改采用国际标准也是采用国际标准的基本方法之一。它是指允许我国标准与国际标准存在技术性差异，并对这些技术性差异进行了清楚地标识和解释。在结构上，我国标准应与相应国际标准相同，但如不影响对两个标准的内容进行比较，则允许改变文本结构。“修改”的标准还可包括“等同”采用下的编辑性修改的内容，其缩写字母代号为 IDT。对于修改采用国际标准“反之亦然原则”不适用。

与国际标准的一致性程度为非等效的国家标准不属于采用国际标准，它是指我国标准与相应国际标准在技术内容和文本结构上均不同，它们之间的差异也未被清楚地标识。其缩写字母代号为 NEQ。

标准化技术委员会是制定国家标准和行业标准的一种重要组织形式，它是一定专业领域内从事全国性标准化工作的技术工作组织。

10.3.2 标准的意义与作用

建立标准化的意义和作用主要表现在以下 10 个方面：

（1）标准化为科学管理奠定了基础。所谓科学管理，就是依据生产技术的发展规律和客观经济规律对企业进行管理，而各种科学管理制度的形成，都是以标准化为基础的。

（2）促进经济全面发展，提高经济效益。标准化应用于科学研究，可以避免在研究上的重复劳动；应用于产品设计，可以缩短设计周期；应用于生产，可使生产在科学的和有序的基础上进行；应用于管理，可促进统一、协调、高效率等。

（3）标准化是科研、生产、使用三者之间的桥梁。一项科研成果，一旦纳入相应标准，就能迅速得到推广和应用。因此，标准化可使新技术和新科研成果得到推广应用，从而促进技术进步。

（4）随着科学技术的发展，生产的社会化程度越来越高，生产规模越来越大，技术要求越来越复杂，分工越来越细，生产协作越来越广泛，这就必须通过制定和使用标 准，来保证各生产部门的活动，在技术上保持高度的统一和协调，以使生产正常进行。所以，我们说标准化为组织现代化生产创造了前提条件。

（5）促进对自然资源的合理利用，保持生态平衡，维护人类社会当前和长远的利益。

（6）合理发展产品品种，提高企业应变能力，以更好地满足社会需求。

（7）保证产品质量，维护消费者利益。

（8）在社会生产组成部分之间进行协调，确立共同遵循的准则，建立稳定的秩序。

（9）在消除贸易障碍、促进国际技术交流和贸易发展、提高产品在国际市场上的竞争能力方面具有重大作用。

（10）保障身体健康和生命安全。大量的环保标准、卫生标准和安全标准制定发布后，用法律形式强制执行，对保障人民的身体健康和生命财产安全具有重大作用。

10.3.3 标准的层次与类别

“标准”实质上就是“规则”，大家做事必须遵循的准则和依据。按适用范围分有“国家标准、行业标准、地方标准和企业标准”；按法律的约束性分有“强制性标准、推荐性标准和标准化指导性技术文件”；按标准的性质分有“技术标准、管理标准和工作标准”；按标准化的对象和作用分有“基础标准、产品标准、方法标准、安全标准、卫生标准和环境保护标准”。

《中华人民共和国标准化法》将标准划分为四个层次，即国家标准、行业标准、地方标准、企业标准。各层次之间有一定的依从关系和内在联系，形成一个覆盖全国又层次分明的标准体系。

（1）国家标准。对需要在全国范围内统一的技术要求，应当制定国家标准。国家标准由国家标准化管理委员会编制计划、审批、编号、发布。国家标准代号为 GB 和 GB/T，其含义分别为强制性国家标准和推荐性国家标准。国家标准在全国范围内适用，其它各级标准不得与之相抵触。国家标准是四级标准体系中的主体。

（2）行业标准。对没有国家标准又需要在全国某个行业范围内统一的技术要求，可以制定行业标准，是专业性、技术性较强的标准。作为对国家标准的补充，当相应的国家标准实施 后，该行业标准应自行废止。行业标准由行业标准归口部门编制计划、审批、编号、发布、管理。行业标准的归口部门及其所管理的行业标准范围，由国务院行政主 管部门审定。部分行业的行业标准代号如下：汽车——QC、石油化工——SH、化工——HG、石油天然气——SY、有色金属——YS、电子——SJ、机械 ——JB、轻工——QB、船舶——CB、

核工业——EJ、电力——DL、商检——SN、包装——BB。推荐性行业标准在行业代号后加“/T”，如 “JB/T”即为机械行业推荐性标准，不加“T”为强制性标准。

（3）地方标准。对没有国家标准和行业标准而又需要在省、自治区、直辖市范围内统一的要求，可以制定地方标准。地方标准的制定范围有：工业产品的安全、卫生要求；药品、兽 药、食品卫生、环境保护、节约能源、种子等法律、法规的要求；其它法律、法规规定的要求。地方标准由省、自治区、直辖市标准化行政主管部门统一编制计划、 组织制定、审批、编号、发布。地方标准在本行政区域内适用，不得与国家标准和行业标准相抵触。国家标准、行业标准公布实施后，相应的地方标准即行废止。 地方标准也分强制性与推荐性。

（4）企业标准。是对企业范围内需要协调、统一的技术要求、管理要求和工作要求所制定的标准。企业产品标准其要求不得低于相应的国家标准或行业标准的要求。企业标准由企业制定，企业标准是企业组织生产，经营活动的依据，由企业法人代表或法人代表授权的主管领导批准、发布。企业产品标准应在发布后 30 日内向政府备案。此外，为适应某些领域标准快速发展和快速变化的需要，于 1998 年规定在四级标准之外，增加一种“国家标准化指导性技术文件”，作为对国家标准的补充，其代号为“GB/Z”。指导性技术文件仅供使用者参考。

根据标准管理的需要，标准种类一般按行业、性质、功能分类。

（1）按行业分类

目前我国按行业归类的标准已正式批准了 57 大类，行业大类的产生过程是：由国务院各有关行政主管部门提出其所管理的行业标准范围的申请报告，经国务院标准化行政主管部门（目前是国家标准化管理委员会）审查确定，同时公布该行业的标准代号。

（2）按标准性质分类

通常按标准的专业性质，将标准划分为技术标准、管理标准和工作标准三大类。 在标准化领域中，对需要统一的技术事项所制定的标准称为技术标准；而对需要协调统一的管理事项所制定的标准叫管理标准；为实现工作（活动）过程的协调，提高工作质量和工作效率，对每个职能和岗位的工作制定的标准为工作标准。

（3）按标准的功能分类

基于社会对标准的需求，为了对常用的量大面广的标准进行管理，通常将重点管理的标准分为：基础标准、产品标准、方法标准、安全标准、卫生标准、环保标准、管理标准。

10.4 我国信息安全标准化工作

我国政府高度重视信息安全标准化工作，在国家政策中对推进信息安全标准化工作做出了明确部署，专门成立了信息安全标准化工作组织机构，发布了“十一五”信息安全标准化工作规划，标准化工作取得了明显成果，标准的基础性、规范性作用进一步加强。

10.4.1 组织结构

1．成立

信息安全标准是我国信息安全保障体系的重要组成部分，是政府进行宏观管理的重要依据。由于信息安全标准关系到国家的安全及经济利益，标准往往成为保护国家利益、促进产业发展的一种重要手段。信息安全标准化是一项涉及面广、组织协调任务重的工作，是一项需要各方面支持和协作的工作。

为了充分发挥生产、使用、科研、教学和监督检验、经销等方面的专家的作用，更好地开展信息安全技术领域的标准化工作，经国家标准化管理委员会批准，我国于 2002 年成立了“全国信息安全标准化技术委员会”，简称信安标委（TC260），由国家标准委直接领导，对口 ISO/IEC JTC1 SC27。其英文名称是“China Information Security Standardization Technical Committee”（英文缩写“CISTC”）。该委员会是在信息安全技术专业领域内，从事信息安全

标准化工作的技术工作组织。委员会负责组织开展国内信息安全有关的标准化技术工作，其主要工作范围包括：安全技术、安全机制、安全服务、安全管理、安全评估等领域的标准化技术工作。

全国信息安全标委会以专家为主体组成，设委员若干名，其中主任委员一人，副主任委员若干人，秘书长一人，副秘书长若干人。

秘书处是委员会的常设机构，负责处理日常工作，设在中国电子技术标准化研究所。

2．职责

信安标委是我国信息安全技术专业领域内从事信息安全标准化工作的专业性技术机构，其主要职责是：（1）在国家有关方针政策指导下，向国家标准化管理委员会提出本专业标准化工作的方针、政策和技术措施的建议。（2）按照国家积极采用国际标准和国外先进标准的政策，制定本专业标准体系表，提出本专业制、修订国家标准的规划和年度计划的建议。（3）根据国家标准化管理委员会批准的计划，协助组织本专业国家标准的制、修订工作，协调有关的标准化技术方面的工作。（4）组织对本专业负责管理的国家标准送审稿的审查工作，提出审查结论或修改意见，并对标准的技术问题负责。定期复审本专业现行国家标准，提出修订、废止或确认的意见。（5）负责本专业国家标准的宣讲、讲解工作。收集对已颁布标准的意见。向国家标准化管理委员会提出本专业标准化成果奖励项目的建议。（6）受国家标准化管理委员会委托，负责对国际标准文件的表决，审查有关的我国提案。组织开展国际标准化技术交流和合作。（7）受有关部门委托在产品质量监督检验、认证等方面，承担本专业范围内产品质量标准的水平评价或认可工作。（8）可接受有关省、市和企业委托，承担本专业企业标准的制定、审查、宣讲和咨询等工作。（9）组织本专业标准化的研究，开展学术活动，组织培训和咨询服务工作。（10）承担国家标准化管理委员会委托办理的与本专业标准化工作有关的其它事宜。

国标委高新函[2004]1 号文决定，自 2004 年 1 月起，各有关部门在申报信息安全国家标准计划项目时，必须经信息安全标委会提出工作意见，协调一致后由信息安全标委会组织申报；在国家标准制定过程中，标准工作组或主要起草单位要与信息安全标委会积极合作，并由信息安全标委会完成国家标准送审、报批工作。

3．工作组

目前，信安标委已启动了 6 个工作组。 WG1 是信息安全标准体系与协调工作组，由国内 13 位知名专家学者组成。WG1 的主要工作任务有：研究信息安全标准体系；跟踪国际标准发展动态；研究信息安全标准需求；研究并提出新工作项目及设立新工作组的建议；协调各工作组项目。

WG2 是涉密信息系统安全保密标准工作组。WG2 的主要工作任务有：研究提出涉密信息系统安全保密标准体系；制定和修订涉密信息系统安全保密标准。

WG3 是密码技术标准工作组。WG3 的主要工作任务有：研究提出密码技术标准体系；研究制定密码算法、密码模块和密钥管理等相关标准。

WG4 是鉴别与授权工作组。WG4 的主要工作任务有：研究制定鉴别与授权标准体系；调研国内相关标准需求；研究制定鉴别与授权标准。

WG5 是信息安全评估工作组。WG5 的主要工作任务有：调研测评标准现状与发展趋势；研究我国统一测评标准体系的思路和框架，提出测评标准体系；研究制订急需的测评标准。

WG7 是信息安全管理工作组。WG7 的主要工作任务有：研究信息安全管理动态，调研国内管理标准需求；研究提出信息安全管理标准体系；制定信息安全管理相关标准。

10.4.2 其他信息安全标准管理机构

除全国信息安全标准化技术委员会负责信息安全国家标准的技术管理外，我国国家保密局负责管理、发布，并强制执行国家保密标准。国家保密标准适用于指导全国各行各业、各

个单位国家秘密的保护工作，具有全国性指导作用，是国家信息安全标准的重要组成部分。国家保密标准与国家保密法规共同构成我国保密管理的重要基础，是保密防范和保密检查的依据，为保护国家秘密的安全发挥了非常重要的作用。

此外，我国还有一些行业标准化组织负责组织制定涉及信息安全的行业标准。这些行业标准化组织主要有：

（1）公安部信息系统安全标准化技术委员会

公安部信息系统安全标准化技术委员会于1999年3月31日经公安部科技局批准正式成立。主要任务是在公安部的领导下，负责规划和制定我国公共安全行业信息安全标准和技术规范，监督技术标准的实施。

（2）中国通信标准化协会网络与信息安全技术工作委员会

中国通信标准化协会于2003年12月成立了网络与信息安全技术工作委员会（TC8），其主要职责是专门组织、研究和制订通信行业网络与信息安全相关的技术标准和技术规范。

10.4.3 国家信息安全标准制定流程

信安标委制定标准的工作程序主要包括如图10-1所示的以下阶段：

（1）根据国家标准制、修订规划和产业需求，提出年度国家标准制、修订项目的建议，报国家标准化管理委员会。

（2）根据国家标准制、修订计划，协助组织计划的实施，指导和督促各工作组进行标准的制、修订工作。

（3）负责工作组在调查研究和试验验证的基础上，提出标准草案征求意见稿（包括附件），分送委员会有关委员和有关单位征求意见，征求意见时间一般为两个月。负责起草单位或工作组对所提意见进行综合分析后，对标准草案进行修改，提出标准送审稿，报送委员会秘书处。

（4）秘书处将标准送审稿送主任委员（或授权的副主任委员）初审后，提交全体委员进行审查（可采用会议形式或函审形式进行）。秘书处在会议前一个月或记名投票前两个月，将标准送审稿（包括附件）提交给审查者。

（5）标准送审稿的审查，原则上应协商一致，如需表决必须有三分之二以上委员同意，并且与会委员必须二分之一以上（会审时未出席会议也未说明意见者，以及函审时未按规定时间投票者按弃权计票）。

（6）对有分歧意见的标准或条款须有不同观点的论证材料。审查标准的投票情况应以书面材料记录在案。如表决通过后，对不同意见的处理还需进行多次投票（具体要看所提意见是否为实质性的意见）。公开征求意见的时间一般截止到下次会议之前。

（7）信安标委通过的标准送审稿，由负责起草单位或工作组根据审查意见进行修改，按有关要求提出标准报批稿及其附件，负责起草单位或工作组应对标准报批稿的技术内容和编写质量负责。

（8）由信安标委秘书处复核并经秘书长签署意见，送主任委员（或授权的副主任委员）审核签字后，送标准起草单位的主管部门，按行政渠道上报国家标准化管理委员会批准发布。

（9）信安标委一般每年召开一次全会，总结工作，检查计划执行情况，检查经费使用情况，研究布置下一年度的工作计划等，并均应以书面形式报告国家标准化管理委员会。全会闭幕期间，由正（或授权的副）主任委员主持委员会的工作。

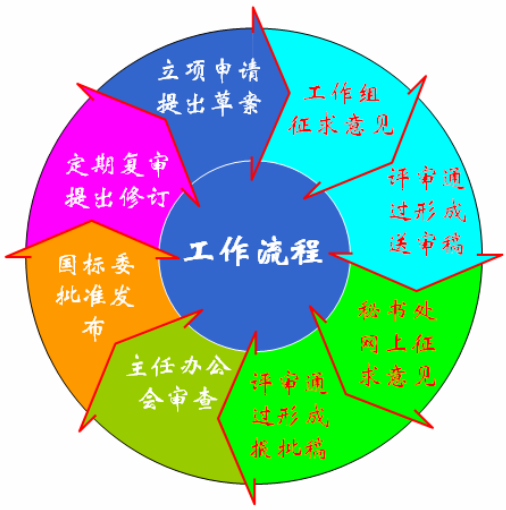


图 10-1　标准制定流程

10.4.4　国家信息安全标准化工作成果

信安标委成立以来，其工作重点是制定以下几方面的标准：信息安全等级保护；网络信任体系建设；信息安全应急处理；信息安全产品测评；信息安全管理。

截至目前，委员会共完成制定信息安全国家标准 76 项（13 项修订标准），有 50 项信息安全标准的研制在进行中。标准在各个范围的分布情况如表 1 所示。

表 10-1　信息安全标准分布情况

	完成标准制定	正在制订标准
信息安全等级保护	9	2
网络信任体系建设	30	19
信息安全产品测评	26	17
信息安全管理标准	10	4
其它应用安全标准	1	8
合　计	76	50

在信安标委的组织下，在社会各界的支持下，经过多年的努力，目前中国已经初步形成了与国际衔接的有中国特色的信息安全标准体系，如图 10-2 所示。

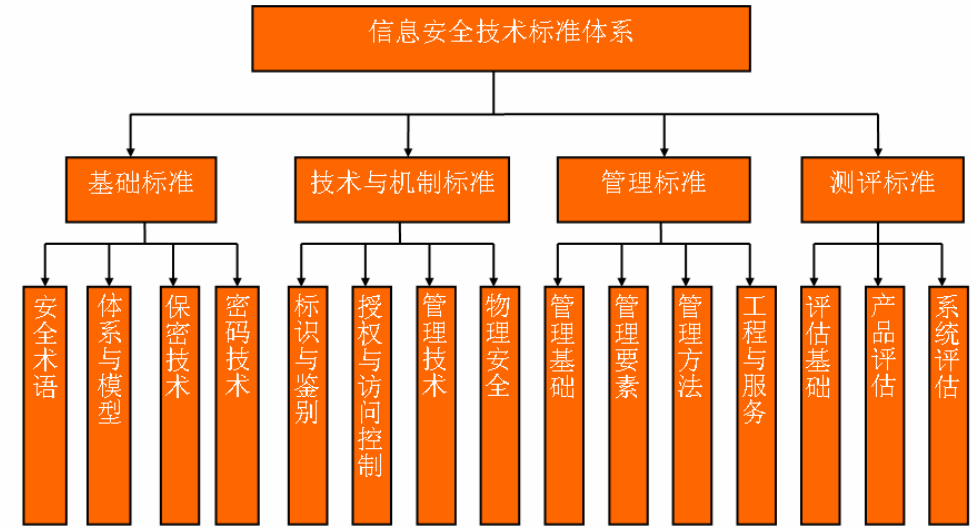


图 10-2　中国信息安全标准体系

这些标准为我国信息系统等级保护、信息安全风险评估、网络信任体系建设、重要信息系统灾难恢复、信息安全应急处理、信息安全产品测评认证和信息安全管理等信息安全重点工作和《电子签名法》实施提供了有效的标准支撑。

此外，我国在积极参与国际交流与合作的基础上，实现了信息安全国际标准化工作的突破，取得了较好的成果。目前，我国的两项标准提案（《信息安全管理体系审核指南》和《基于三元对等鉴别的访问控制方法》）被 ISO/IEC JTC1 SC27 接纳作为新国际标准项目，有 3 名中国专家作为编制人参与国际标准《信息安全事件管理指南》的联合编辑。2009 年 5 月，我国成功举办了 2009 年度 ISO/IEC JTC1 SC27 工作组会议及全体会议，提高了我国在国际信息安全标准化领域的影响力，进一步提升了我国在国际信息安全标准化组织中地位

10.4.5 工作规划

2007 年 5 月，国家标准委和原国务院信息办联合发布了《国家信息安全标准化“十一五”规划》。该规划提出，到“十一五”末期，基本建立适应信息安全保障体系建设需求的信息安全标准体系；完成 150 项国家标准的制定；自主制定高质量国家标准比例达到 40%；提高实质参与国际标准化活动的水平，在制定国际标准上取得突破。

《国家信息安全标准化“十一五”规划》部署了“十一五”期间中国信息安全标准化工作的主要任务：

（1）开展标准战略与基础理论研究

进一步加强信息安全标准战略与基础理论研究，密切跟踪信息安全保障技术发展动态，做好顶层设计和整体规划，构建一个结构合理、科学实用、能与国际衔接、体现自主可控的信息安全标准体系，指导信息安全标准制定工作。

（2）加快急需标准的制定

结合国家信息安全监管、电子政务与电子商务等重大工程建设和产业发展的信息安全标准需求，重点做好基础类、管理类和系统类标准的研究制定，为信息安全保障体系建设提供支撑。

每年研究制定 30 项左右国家标准，到“十一五”末完成 150 项国家标准的制定，其中自主制定标准 60 项。

（3）做好标准的推广实施

进一步加强标准的推广应用和检查力度，提高标准应用效果，重点做好新颁布国家标准的推广应用工作。建立健全标准服务机制，整合优化信息安全标准化资源，统一规划和建设国家信息安全标准化信息网络服务平台体系，提供高效、便捷、准确的信息安全标准信息服务，全面推进信息安全标准的实施应用。

（4）积极参与国际标准化活动

建立参与国际标准化活动的长效机制，积极参加国际标准化会议，加强国际、双边、多边和区域标准化交流与合作，加强国际和国外先进标准研究，推进国际标准采用，建立稳定的国际标准化人才队伍，争取国际标准化活动中的话语权，提高实质参与国际信息安全标准化活动的能力。“十一五”期间，力争提交 2-3 项国际标准提案，成为 1-2 项国际标准的编辑。争取在中国举办 1 到 2 次国际标准工作会议和区域信息安全标准工作会议。

《国家信息安全标准化“十一五”规划》提出了“十一五”期间中国信息安全标准化工作的 16 个方面的重点项目，如表 10-2 所示。

表 10-2 “十一五”期间重点信息安全标准项目

信息安全等级保护有关标准	涉密信息系统安全保密标准	密码技术和网络信任体系标准	电子政务信息安全标准
电子商务信息安全标准	信息安全政府监管有关标准	信息安全管理体系标准	信息安全应急与灾备有关标准
信息安全服务管理标准	信息安全测评标准	信息安全保障指标与评价体系	可信计算技术标准
无线通信和移动通信安全标准	通讯社及广播电视等新闻发布系统安全标准	信息安全相关的生物特征识别标准	信息安全标准体系

10.5 国外信息安全标准化组织及其工作进展

国际上的信息安全标准化工作兴起于二十世纪 70 年代中期，80 年代有了较快的发展，90 年代引起了世界各国的普遍关注。目前，与信息安全标准化有关的主要国际组织有：国际标准化组织（ISO）、国际电工委员会（IEC）、国际电信联盟（ITU）、Internet 工程任务组（IETF）等。

10.5.1 信息安全标准化组织

国际标准化组织（ISO）于 1947 年 2 月 23 日正式开始工作，ISO 与 IEC（国际电工委员会）联合成立了第一技术委员会（JTC1），负责信息技术标准化，其下属第 27 分委会（SC27）是安全技术分委员会，其前身是 SC20（数据加密分技术委员会），主要从事信息技术安全的一般方法和技术的标准化工作。SC27 下设 5 个工作组，主要负责研究和制定信息安全管理体系、密码学与安全控制、信息安全评估、安全控制与服务以及身份管理与隐私保护等领域的信息安全国际标准。目前 SC27 共有 P 成员（正式成员）国家 40 个，O 成员（观察成员）国家 12 个。

国际电工委员会（IEC）正式成立于 1906 年 10 月，是世界上成立最早的专门国际标准化机构。在信息安全标准化方面，主要与 ISO 联合成立了 JTC1 下 分委员会外，还在电信、电子系统、信息技术和电磁兼容等方面成立技术委员会，如 TC56 可靠性、TC74IT 设备安全和功效、TC77 电磁兼容、 TC108 音频/视频、信息技术和通讯技术电子设备的安全等，并制定相关国际标准，如信息技术设备安全（IEC60950）等。

国际电信联盟（ITU）成立于 1865 年 5 月 17 日，所属的 SG17 组，主要负责研究通信系统安全标准。SG17 组主要研究的有：通信安全项目、安全架构和框架、计算安全、安全管理、用于安全的生物测定、安全通信服务。此外 SG16 和下一代网络核心组也在通信安全、H323 网络安全、下一代网络安全等标准方面进行了研究。目前 ITU-T 建议书中大约有 40 多个都是与通信安全有关的标准。

Internet 工程任务组（IETF）始创于 1986 年，其主要任务是负责互联网相关技术规范的研发和制定。目前，IETF 已成为全球互联网界最具权威的大型技术研究组织。IETF 标准制定的具体工作由各个工作组承担，工作组分成八个领域，分别是 Internet 路由、传输、应用领域等等，著名的 IKE 和 IPSec 都在 RFC 系列之中，还有电子邮件，网络认证和密码标准，也包括了 TLS 标准和其它的安全协议标准。

国际电报和电话咨询委员会（CCITT）是一个联合国条约组织，属于国际电信联盟，由主要成员国的邮政、电报和电话当局组成，主要从事涉及通信领域的接口和通信协议的制定，与 ISO 密切合作进行国际通信的标准化工作，在数据通信范围内的工作体现于 V 系列和 X 系列建议书。

国际信息处理联合会第十一技术委员会（IFIPTC11）是国际上有重要影响的有关信息系统安全的国际组织，公安部代表我国参加该组织的活动，该组织每年举行一次信息安全的国际研讨会。该组织机构包括安全管理工作组、办公自动化安全工作组、数据库安全工作组、密码工作组、系统完整性与控制工作组、计算机事务处理工作组、计算机安全法律工作组和计算机安全教育工作组。

电气和电子工程师学会（IEEE）是一个由电气和电子工程师组成的世界上最大的专业性学会，划分成许多部门。1980 年 2 月，IEEE 计算机学会建立了一个委员会负责制定有关网络的协议标准（802.1～9），包括高层接口、逻辑链路控制、CSMA/CD 网、令牌总线网、令牌环网、城域网、宽带技术咨询组、光纤技术咨询组、数据和话音综合网络等标准。

欧洲计算机制造商协会（ECMA）是包括美国在欧洲供应计算机的厂商在内组成的组织，致力于适用于计算机技术的各种标准的制定和颁布，在 ISO 和 CCITT 中是一个没有表决权的成员。

美国国家标准局（NBS）属于美国商业部的一个机构，现在的工作由美国商业部国家标准与技术研究院（NIST）进行，制订美国联邦信息处理标准。NIST 还与 NSA 紧密合作，在 NSA 的指导监督下，制定计算机信息系统的技术安全标准。它的工作一般以 NIST 出版物（FIPSPUB）和 NIST 特别出版物（SPECPUB）等形式发布。它制定的信息安全规范和标准很多，主要涉及访问控制和认证技术、评价和保障、密码、电子商务、一般计算机安全、网络安全、风险管理、电讯和联邦信息处理标准等。该机构比较有影响的工作是制定公布了美国国家数据加密标准 DES，参加了美国、加拿大、英国、法国、德国、荷兰等国制定的信息安全的通用评价准则（CC），在 1993 年制定了密钥托管加密标准 EES。美国近年来在 AES 算法征集方面的活动以及新的散列函数征集活动均由 NIST 负责组织。

美国国家标准协会（ANSI）是由制定标准和使用标准的组织联合组成的非盈利的非政府的民间机构，由全美 1000 多家制造商、专业性协会、贸易协会、政府和管理团体、公司和用户协会组成，是美国自发的制定与计算机工业有关的各种标准的统筹交流组织。

10.5.2 信息安全评估国际标准的发展

从 20 世纪 80 年代开始，世界各国相继制订了多个信息技术安全评价标准。这些标准中美国国防部 1985 年发布的《可信计算机系统评估准则》（TCSEC）为最早。本书前面曾说明过该标准。

TCSEC 标准发布以后，各国在 TCSEC 标准的基础上结合本国国情相继发布了自己的信息安全技术标准。这些标准吸收了 TCSEC 的经验和教训，从技术上说都有一定的进步。如 90 年代初由欧盟四国（法国、德国、芬兰、英国）联合开发了发布的信息技术安全评价标准（ITSEC）。ITSEC 定义了七个安全级别：不能充分满足保证（E0）、功能测试（E1）、数字化测试（E2）、数字化测试分析（E3）、半形式化分析（E4）、形式化分析（E5）、形式化验证（E6）。

1993 年，加拿大发布了《加拿大可信计算机产品评价标准》（CTCPEC）。同年，美国对可信计算机系统评估准则（TCSEC）作了补充和修改，国家标准局和国家安全局合作制定了信息技术安全联邦（Federal）标准（FC），明确了由用户提供其系统安全保护需求的详细框架，产品厂商定义产品的安全功能、安全目标等，但其有很多缺陷，只是一个过渡准则。这些标准基本上都采用了 TCSEC 的安全框架和模式，将信息系统的安全（可信）性分成不同的等级，并规定了不同的等级应实现的安全功能或安全措施。

随着贸易全球化和经济一体化的发展，更加统一的信息安全评估准则呼之欲出。早在20世纪九十年代初，为了能集中世界各国安全评估准则的优点，集合成单一的、能被广泛接受的信息技术评估准则，国际标准化组织就已就着手编写国际性的信息安全评估准则，但由于任务过于庞大以及协调困难，该工作一度进展缓慢。

直到1993年6月，在6国7方（英、加、法、德、荷、美国的国家安全局及国家标准和技术研究所）的合作下，前述的几个评估标准终于走到了一起，形成了《信息技术安全通用评估准则》，简称CC（Common Criteria）。CC的1.0版于1996年发布，2.0版于1998年发布，1999年，现在的CC2.1版问世，并于1999年12月被ISO批准为国际标准，编号ISO/IEC 15408:1999《信息技术 安全技术 信息技术安全评估准则》。我国在2001年将CC等同采用为国家标准，以编号GB/T 18336-2001发布。2005年，ISO/IEC 15408:2005取代了ISO/IEC 15408:1999。相应地，我国在2008年完成了GB/T 18336-2001的更新工作，发布了GB/T 18336-2008。

图10-3是对国际上信息安全评估标准发展的概括。

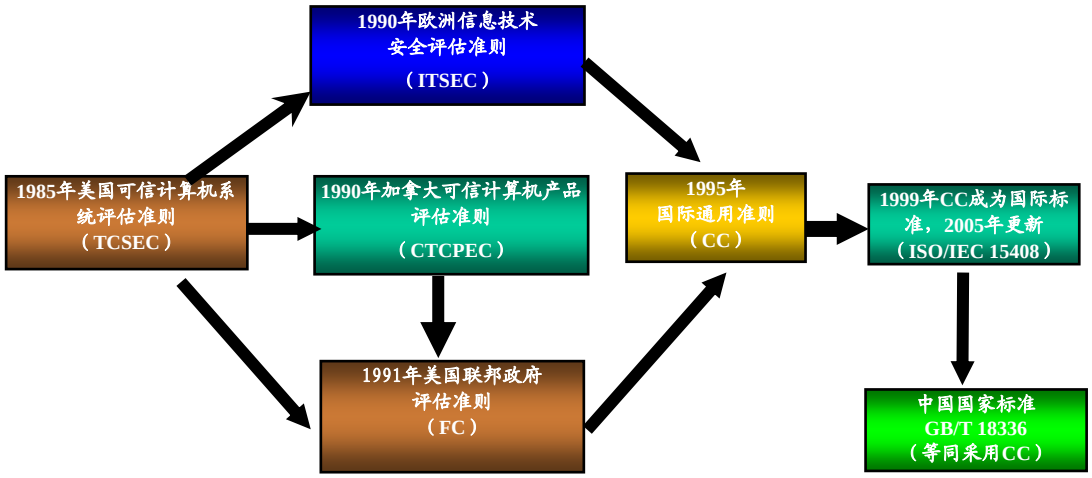


图 10-3　信息安全评估标准的发展

CC 吸收了各先进国家对现代信息系统安全的经验和知识，对信息安全的发展与应用带来了深刻影响。它分为三部分，其中第 1 部分是介绍 CC 的基本概念和基本原理，第 2 部分提出了安全功能要求，第 3 部分提出了安全保证要求。后两部分构成了 CC 安全要求的全部：安全功能要求和安全保证要求，其中安全保证的目的是为了确保安全功能的正确性和有效性，这是从 ITSEC 和 CTCPEC 中吸收的。同时 CC 也还从 FC 中吸收了保护轮廓（PP）的概念，从而为 CC 的应用和发展提供了最大可能的空间和自由度。

CC 的功能要求和保证要求均以类-族-组件（class-family-component）的结构表述。“类”用于安全要求的最高层次归类。一个类中所有成员关注同一个安全焦点，但覆盖的安全目的范围不同，类的成员被称为族。族是若干组安全要求的组合，这些要求共享同样的安全目的，但在侧重点和严格性上有所区别，族的成员被称为组件。一个组件描述一组特定的安全要求，它是 CC 结构中安全要求的最小可选集合。一个族中的组件集合，可以按安全要求强度或能力递增的顺序进行描述，这些安全要求具有相同用途；在部分族也可以不区分层次的方式来描述。CC 发展很快，各个版本之间有的差异较大。以 ISO/IEC15408:2005 为例，前者包括 11 个功能类（安全审计、通信、密码支持、用户数据保护、标识和鉴别、安全管理、私密性、TSF 保护、资源利用、TOE 访问、可信路径/信道），后者包括 7 个保证类（配置管理、交付和运行、开发、指导性文档、生命周期支持、测试、脆弱性评定）。

保证类、族和每一个保证族的缩写都在表10-3中列出。

表 10-3　CC 保证族细目分类和对应关系

保证类	保证族	缩写名
ACM 类：配置管理	CM 自动化	ACM_AUT
	CM 能力	ACM_CAP
	CM 范围	ACM_SCP
ADO 类：交付和运行	交付	ADO_DEL
	安装、生成和启动	ADO_IGS
ADV 类：开发	功能规范	ADV_FSP
	高层设计	ADV_HLD
	实现表示	ADV_IMP
	TSF 内部	ADV_INT
	低层设计	ADV_LLD
	表示对应性	ADV_RCR
	安全策略模型	ADV_SPM
AGD 类：指导性文档	管理员指南	AGD_ADM
	用户指南	AGD_USR
ALC 类：生命周期支持	开发安全	ALC_DVS
	缺陷纠正	ALC_FLR
	生命周期定义	ALC_LCD
	工具和技术	ALC_TAT

ATE 类：测试	覆盖	ATE_COV
	深度	ATE_DPT
	功能测试	ATE_FUN
	独立测试	ATE_IND
AVA 类：脆弱性评定	隐蔽信道分析	AVA_CCA
	误用	AVA_MSU
	TOE 安全功能强度	AVA_SOF
	脆弱性分析	AVA_VLA

CC 通过对安全保证（而非安全功能）的评估而划分安全等级，每一等级对保证功能的要求各不相同。安全等级增强时，对保证组件的数目或者同一保证的强度的要求会增加。

CC 的安全等级简称 EAL（评估保证级），共分 7 级 EAL，安全等级由 EAL1 到 EAL7 级逐渐提高，分别为：

- EAL7：形式化验证的设计和测试；
- EAL6：半形式化验证的设计和测试；
- EAL5：半形式化设计和测试；
- EAL4：系统地设计、测试和复查；
- EAL3：系统地测试和检查；
- EAL2：结构测试；
- EAL1：功能测试。

图 10-3 所示的各项信息安全评估标准以及 GB 17859-1999 之间，存在着一个大致的安全级别对照关系，如表 10-4 所示。之所以称其为“大致的”，是因为 ITSEC 和 CC 等标准的关注对象已经超出了 TCSEC 的范围，而且这些标准的安全等级不再是简单针对安全功能的评估，这种情况使得这几部标准的比较缺乏参照系。因此表 10-4 中反映的对照关系不是很精确，只能作为一种定性参考。

表 10-4　各信息安全评估标准间的级别对照

Information Technology Security Common Criteria 国际 CC 标准	Trusted Computer System Evaluation Criteria 美国 TCSEC	Information Technology Security Evaluation Criteria 欧洲 ITSEC	Canada Trusted Computer Product Evaluation Criteria 加拿大 CTCPEC	中国 GB 17859-1999
--	D:低级保护	E0	T0	--
EAL1-功能测试	--	--	T1	--
EAL2-结构测试	C1:自主安全保护	E1	T2	1:用户自主保护级
EAL3-方法测试和检验	C2:受控访问保护	E2	T3	2:系统审计保护级
EAL4-方法设计，测试和复查	B1:标记安全保护	E3	T4	3:安全标记保护级
EAL5-半形式化设计和测试	B2:结构化保护	E4	T5	4:结构化保护级
EAL6-半形式化验证的设计和测试	B3:安全区域	E5	T6	5:访问验证保护级
EAL7-形式化验证的设计和测试	A1:验证设计	E6	T7	--

虽然 CC 有很多优点，世界上正有越来越多的国家建立了基于 CC 的国家信息安全认证体制，但 CC 也有一些固有的局限性。从 CC 的应用来说，基于 CC 的评估需要耗费大量的事件和资金，例如 EAL4 级评估所需的时间一般为 10-25 个月，这样长的时间是很多产品生产商所无法忍受的。而即使经过了漫长的评估，所获得的评估报告也可能对用户采购满足其需求的产品而言缺少实际意义。近几年来，围绕 CC 的不足，已经有了很多的讨论，CC 的管理方已经宣布着手制定全新的 CC 4.0 版本，以谋求 CC 的自我革新。

CC 所提出的安全要求缺少严格的数学模型的支持，这一点尤应引起注意。虽然美国早已宣布其在产品评估中已经由 CC 取代了 TCSEC，但后者有 Bell & La Padula 模型的支持，其安全功能可以得到完善的解释，对于描述高安全等级的信息系统更加有优势。因此，对 CC 和 TCSEC 的优劣问题，不能简单一概而论。在信息系统安全等级保护建设中，应努力

运用 TCSEC 的设计思想，科学构建网络环境下的“可信计算基”（TCB），在高安全等级信息系统内实现强制访问控制和结构化保护功能。

10.5.3 ISO/IEC JTC1 SC27 主要活动

经过多年发展，目前 ISO/IEC JTC1 SC27 已经成为信息安全领域最权威和得到国际最广泛认可的标准化组织，为信息安全领域的标准化工作做出了巨大贡献。

SC27 内现有 5 个工作组，分别为信息安全管理体系工作组（WG1）、密码与安全机制工作组（WG2）、安全评估准则工作组（WG3）、安全控制与服务工作组（WG4）、身份管理与隐私技术工作组（WG5）。

表 10-5 给出了截至 2008 年上半年，ISO/IEC JTC1 SC27 内各标准的发展情况。

表 10-6　ISO/IEC JTC1 SC27 标准动态

标准号	标准名称（英文）	标准名称（中文）	标准版本	修订	备注
ISO/IEC TR 13335-3	Guidelines for the management of IT security - Part 3: Techniques for the management of IT security	IT 安全管理指南 — 第三部分：IT 安全管理技术		修订	
ISO/IEC TR 13335-4	Guidelines for the management of IT security - Part 4: Selection of safeguards	IT 安全管理指南 — 第四部分：安全措施选择		修订	
ISO/IEC TR 13335-5	Guidelines for the management of IT security - Part 51: Management guidance on network security	IT 安全管理指南 — 第五部分：网络安全管理指南		修订	
ISO/IEC 13335-1	Management of information and communications technology security - Part 1: Concepts and models for Information and Communications Technology (ICT) security management	信息与通信技术安全管理 — 第一部分：信息与通信技术（ICT）安全管理的概念和模型			
ISO/IEC 13335-2	Management of information and communications technology security - Part 2: Information security risk management	信息与通信技术安全管理 — 第二部分：信息安全风险管理			
ISO/IEC 27000	Information security management systems - Overview and vocabulary	信息安全管理体系—概述和词汇	3CD		
ISO/IEC 27001	Information security management systems - Requirements	信息安全管理体系 — 要求			
ISO/IEC 27002	Code of practice for information security management	信息安全管理实用规则	2		
ISO/IEC 27003	Information security management system implementation guidance	信息安全管理体系实现指南	4WD		
ISO/IEC 27004	Information security management measurements	信息安全管理测量	2CD		
ISO/IEC 27005	Information security risk management	信息安全风险管理	2FCD		
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems	信息安全管理体系审核认证机构的要求			
ISO/IEC 27007	Guidelines for information security management systems auditing	信息安全管理体系审核指南	NP		
ISO/IEC 27011	Information security management guidelines for telecommunications organizations based on ISO/IEC 27002	基于 ISO/IEC 27002 的远程通信组织信息安全管理指南	FCD		ITU-T X.1051
ISO/IEC 7064	Check character systems	校验字符系统	2		
ISO/IEC 9796-1	Digital signature schemes giving message recovery - Part 1: Mechanisms using redundancy	带消息恢复的数字签名机制 — 第一部分：使用冗余的机制			
ISO/IEC 9796-2	Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms	带消息恢复的数字签名机制 — 第二部分：基于整数因数分解的机制	2		
ISO/IEC 9796-3	Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms	带消息恢复的数字签名机制 — 第三部分：基于离散对数的机制	2		
ISO/IEC 9796-4	Digital signature schemes giving message recovery - Part 3: Discrete logarithm based mechanisms	带消息恢复的数字签名机制 — 第四部分：基于离散对数的机制			ISO/IEC 9796-3 的前身
ISO/IEC 9797-1	Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher	消息鉴别码 — 第一部分：使用块密码的机制		修订	
ISO/IEC 9797-2	Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function	消息鉴别码 — 第二部分：使用专用散列函数的机制		修订	
ISO/IEC 9797-3	Message Authentication Codes (MACs) - Part 3: Mechanisms using a universal hash function	消息鉴别码 — 第三部分：使用通用散列函数的机制	1 WD		
ISO/IEC	Entity authentication - Part 1: General	实体鉴别 — 第一部分：概	2		

9798-1		要			
ISO/IEC 9798-2	Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms	实体鉴别 — 第二部分：使用对称加密算法的机制	2	修订	
ISO/IEC 9798-3	Entity authentication – Part 3: Mechanisms using digital signature techniques	实体鉴别 — 第三部分：使用数字签名技术的机制	2		
ISO/IEC 9798-4	Entity authentication – Part 4: Mechanisms using a cryptographic check function	实体鉴别 — 第四部分：使用密码检查功能的机制	2		
ISO/IEC 9798-5	Entity authentication – Part 5: Mechanisms using zero-knowledge techniques	实体鉴别 — 第五部分：使用零知识技术的机制	2		
ISO/IEC 9798-6	Entity authentication – Part 6: Mechanisms using manual data transfer	实体鉴别 — 第六部分：使用手工数据传输的机制			
ISO/IEC 10116	Modes of operation for an n-bit block cipher algorithm	n 比特块密码算法操作模式	3		
ISO/IEC 10118-1	Hash-functions – Part 1: General	散列函数 — 第一部分：概要	2		
ISO/IEC 10118-2	Hash-functions – Part 2: Hash-functions using an n-bit block cipher	散列函数 — 第二部分：使用 n 比特块密码的散列函数	2	修订	
ISO/IEC 10118-3	Hash-functions – Part 3: Dedicated hash-functions	散列函数 — 第三部分：专用的散列函数	3		
ISO/IEC 10118-4	Hash-functions – Part 4: Hash-functions using modular arithmetic	散列函数 — 第四部分：使用模算法的散列函数		修订	
ISO/IEC 11770-1	Key management – Part 1: Framework	密钥管理 — 第一部分：框架			
ISO/IEC 11770-2	Key management – Part 2: Mechanisms using symmetric techniques	密钥管理 — 第二部分：使用对称技术的机制		修订	
ISO/IEC 11770-3	Key management – Part 3: Mechanisms using asymmetric techniques	密钥管理 — 第三部分：使用非对称技术的机制		修订	
ISO/IEC 11770-4	Key management – Part 4: Mechanisms based on weak secrets	密钥管理 — 第四部分：基于弱秘密的机制			
ISO/IEC 13888-1	Non-repudiation – Part 1: General	抗抵赖 — 第一部分：概要	2		
ISO/IEC 13888-2	Non-repudiation – Part 2: Mechanisms using symmetric techniques	抗抵赖 — 第二部分：使用对称技术的机制		修订	
ISO/IEC 13888-3	Non-repudiation – Part 3: Mechanisms using asymmetric techniques	抗抵赖 — 第三部分：使用非对称技术的机制		修订	
ISO/IEC 14888-1	Digital signatures with appendix – Part 1: General	带附录的数字签名 — 第一部分：概要		修订	
ISO/IEC 14888-2	Digital signatures with appendix – Part 2: Identity-based mechanisms	带附录的数字签名 — 第二部分：基于身份的机制		修订	
ISO/IEC 14888-3	Digital signatures with appendix – Part 3: Certificate-based mechanisms	带附录的数字签名 — 第三部分：基于证书的机制	2		
ISO/IEC 15946-1	Cryptographic techniques based on elliptic curves – Part 1: General	基于椭圆曲线的密码技术 — 第一部分：概要		修订	
ISO/IEC 15946-3	Cryptographic techniques based on elliptic curves – Part 3: Key establishment	基于椭圆曲线的密码技术 — 第三部分：密钥建立			
ISO/IEC 15946-5	Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation	基于椭圆曲线的密码技术 — 第五部分：椭圆曲线产生	1 CD		
ISO/IEC 18014-1	Time-stamping services – Part 1: Framework	时间戳服务 — 第一部分：框架		修订	
ISO/IEC 18014-2	Time-stamping services – Part 2: Mechanisms producing independent tokens	时间戳服务 — 第二部分：产生独立令牌的机制		修订	
ISO/IEC 18014-3	Time-stamping services – Part 3: Mechanisms producing linked tokens	时间戳服务 — 第三部分：产生连环令牌的机制			
ISO/IEC 18031	Random bit generation	随机比特产生			
ISO/IEC 18032	Prime number generation	素数产生			
ISO/IEC 18033-1	Encryption algorithms – Part 1: General	加密算法 — 第一部分：概要			
ISO/IEC 18033-2	Encryption algorithms – Part 2: Asymmetric ciphers	加密算法 — 第二部分：非对称密码			
ISO/IEC 18033-3	Encryption algorithms – Part 3: Block ciphers	加密算法 — 第三部分：块密码			
ISO/IEC 18033-4	Encryption algorithms – Part 4: Stream ciphers	加密算法 — 第四部分：流密码			
ISO/IEC 19772	Authenticated encryption mechanisms	鉴别加密机制	3 CD		
ISO/IEC 15292	Protection profile registration procedures	保护轮廓注册规程			
ISO/IEC 15408-1	Evaluation criteria for IT security – Part 1: Introduction and general model	IT 安全评估准则 — 第一部分：介绍和一般模型	2	修订	
ISO/IEC	Evaluation criteria for IT security – Part 2:	IT 安全评估准则 — 第二	2	修	

15408-2	Security functional requirements	部分：安全功能要求		订	
ISO/IEC 15408-3	Evaluation criteria for IT security – Part 3: Security assurance requirements	IT 安全评估准则 — 第三部分：安全保证要求	2	修订	
ISO/IEC TR 15443-1	A framework for IT security assurance – Part 1: Overview and framework	IT 安全保证框架 — 第一部分：概述和框架			
ISO/IEC TR 15443-2	A framework for IT security assurance – Part 2: Assurance methods	IT 安全保证框架 — 第二部分：保证方法			
ISO/IEC TR 15443-3	A framework for IT security assurance – Part 3: Analysis of assur ance methods	IT 安全保证框架 — 第三部分：保证方法的分析			
ISO/IEC TR 15446	Guide for the production of protection profiles and security targets	保护轮廓和安全目标产生指南		修订	
ISO/IEC 18045	Evaluation methodology for IT security	IT 安全评价方法		修订	
ISO/IEC 19790	Security requirements for cryptographic modules	密码模块安全要求			
ISO/IEC TR 19791	Security assessment for operational systems	运行系统安全评估			
ISO/IEC 19792	Security evaluation and testing of biometrics	生物特征鉴别的安全评价和测试	FCD		
ISO/IEC 21827	Systems security engineering-Capability maturity model	系统安全工程—能力成熟度模型			
ISO/IEC 24759	Test requirements for cryptographic modules	密码模块测试要求	FCD		
ISO/IEC 29128	Verification of cryptographic protocols	密码协议验证	NP		
ISO/IEC TR 14516	Guidelines on the use and management of Trusted Third Party services	可信第三方（TTP）服务的使用和管理指南		修订	ITU-T X.842
ISO/IEC 15816	Security information objects for access control	访问控制的安全信息客体			ITU-T X.841
ISO/IEC 15945	Specification of TTP services to support the application of digital signatures	支持数字签名应用的 TTP 服务规范			ITU-T X.843
ISO/IEC 18028-1	IT network security – Part 1: Network security management	IT 网络安全 — 第一部分：网络安全管理		修订	27033-1
ISO/IEC 18028-2	IT network security – Part 2: Network security architecture	IT 网络安全 — 第二部分：网络安全体系结构		修订	27033-2
ISO/IEC 18028-3	IT network security – Part 3: Securing communications between networks using security gateways	IT 网络安全 — 第三部分：使用安全网关的网间安全通信		修订	27033-4
ISO/IEC 18028-4	IT network security – Part 4: Securing remote access	IT 网络安全 — 第四部分：安全远程访问		修订	27033-5
ISO/IEC 18028-5	IT network security – Part 5: Securing communications across networks using virtual private networks	IT 网络安全 — 第五部分：使用虚拟专用网的跨网安全通信		修订	27033-6
ISO/IEC 18043	Selection, deployment and operations of intrusion detection system	入侵检测系统（IDS）的选择、开发和操作			
ISO/IEC TR 18044	Information security incident management	信息安全事件管理			
ISO/IEC 24762	Guidelines for ICT Disaster Recovery Services	信息与通信技术（ICT）灾难恢复服务指南	FDIS		
ISO/IEC 27031-1	ICT readiness for business continuity – Part 1: Overview of ICT Readiness for Business Continuity	业务连续性的 ICT 准备就绪 — 第一部分：业务连续性的 ICT 准备就绪概述	NP		
ISO/IEC 27031-2	ICT readiness for business continuity – Part 2: Management Framework	业务连续性的 ICT 准备就绪 — 第二部分：管理框架	NP		
ISO/IEC 27031-3	ICT readiness for business continuity – Part 3: Threat Monitoring and Detection	业务连续性的 ICT 准备就绪 — 第三部分：威胁监视与检测	NP		
ISO/IEC 27031-4	ICT readiness for business continuity – Part 4: Vulnerability Management	业务连续性的 ICT 准备就绪 — 第四部分：脆弱性管理	NP		
ISO/IEC 27031-5	ICT readiness for business continuity – Part 5: Incident Management	业务连续性的 ICT 准备就绪 — 第五部分：事件管理	NP		
ISO/IEC 27031-6	ICT readiness for business continuity – Part 6: Services	业务连续性的 ICT 准备就绪 — 第六部分：服务	NP		
ISO/IEC 27031-7	ICT readiness for business continuity – Part 7: Testing and Measurement	业务连续性的 ICT 准备就绪 — 第七部分：测试与测量	NP		
ISO/IEC 27031-8	ICT readiness for business continuity – Part 8: Assurance	业务连续性的 ICT 准备就绪 — 第八部分：保证	NP		
ISO/IEC 27032	Guidelines for Cybersecurity	网络空间安全指南	NP		
ISO/IEC 27033-1	Network security – Part 1: Guidelines for network security	网络安全 — 第一部分：网络安全指南			
ISO/IEC	Network security – Part 2: Guidelines for the	网络安全 — 第二部分：网			

27033-2	design and implementation of network security	络安全设计和实施指南			
ISO/IEC 27033-3	Network security – Part 3: Reference Networking Scenarios – Risks, design techniques and control issues Issues	网络安全 — 第三部分：参考联网场景 — 风险、设计技术和控制问题			
ISO/IEC 27033-4	Network security – Part 4: Security communications between networks using security gateways – Risks, design techniques and control issues Issues	网络安全 — 第四部分：使用安全网关的网间安全通信 — 风险、设计技术和控制问题			
ISO/IEC 27033-5	Network security – Part 5: Securing remote access – Risks, design techniques and control issues Issues	网络安全 — 第五部分：安全远程访问 — 风险、设计技术和控制问题			
ISO/IEC 27033-6	Network security – Part 6: Securing communications across networks using virtual private networks – Risks, design techniques and control issues Issues	网络安全 — 第六部分：使用虚拟专用网的跨网安全通信 — 风险、设计技术和控制问题			
ISO/IEC 27033-N(≥7)	Network security – Part N(≥7): Guidelines for securing specific networking technology - Risks, design techniques and control issues	网络安全 — 第 N（≥七）部分：特定联网技术的安全指南 — 风险、设计技术和控制问题			
ISO/IEC 27034-1	Application security – Part 1: Guidelines for application security	应用安全 — 第一部分：应用安全指南	NP		
ISO/IEC 27034-2	Application security – Part 2: Application Security Lifecycle	应用安全 — 第二部分：应用安全生存周期	NP		
ISO/IEC 27034-3	Application security – Part 3: Architecture, Design, and Development	应用安全 — 第三部分：体系结构、设计和开发	NP		
ISO/IEC 27034-4	Application security – Part 4: Protocols and Data Structure	应用安全 — 第四部分：协议和数据结构	NP		
ISO/IEC 27034-5	Application security – Part 5: Application Security Assurance	应用安全 — 第五部分：应用安全保证	NP		
ISO/IEC 27034- N(≥6)	Application security – Part N(≥6): Security guidance for specific application types, e.g., Web Applications; N-Tier Client/Server Applications	应用安全 — 第 N（≥六）部分：特定应用类型的安全指南，例如，Web 应用、N 层客户端/服务器应用	NP		
ISO/IEC 24745	Biometric template protection	生物特征模板保护	3 WD		
ISO/IEC 24760	A framework for identity management	身份管理框架	3 WD		
ISO/IEC 24761	Authentication context for biometrics	生物特征鉴别背景	3 CD		
ISO/IEC 29100	A privacy framework	隐私保护框架	2 WD		
ISO/IEC 29101	A privacy reference architecture	隐私保护参考体系结构	NP		
ISO/IEC 29115	Entity authentication assurance	实体鉴别保证	1 WD		

说明：CD：委员会草案；FCD：最终委员会草案；FDIS：最终国际标准草案；NP：新项目建议；WD：工作组草案。

本章小结

信息安全立法和标准化相关知识是信息安全领域内的一个重要的知识单元。本章介绍了法律和标准化的基础知识，概述了我国信息安全法律体系的现状和有关工作进展，提供了国内外信息安全标准化工作的概况。

本章内容主要有：

（1）法律基础

法是由一定社会物质生活条件所决定的，由国家制定和认可的，并由国家强制力保证实施的具有普遍约束力的行为规范的总和。法的目的在于维护、巩固和发展一定的社会关系和社会次序。根据《中华人民共和国立法法》，我国的统一而又分层次的立法体制包括以下几个层面：全国人大及其常委会行使国家立法权，制定的法律；国务院制定的行政法规；省、自治区、直辖市的人大及其常委会制定的地方性法规；较大的市（包括省、自治区人民政府所在地的市、经济特区所在地的市和经国务院批准的较大的市）的人大及其常委会制定的地方性法规；经济特区所在地的省、市的人大及其常委会制定的法规，在经济特区范围内实施；自治区、自治州、自治县的人大制定的自治条例和单行条例；国务院各部、各委员会、中国人民银行、审计署和具有行政管理职能的直属机构制定的部门规章；省、自治区、直辖市和较大的市的人民政府制定的地方政府规章。

下位阶的法的规范不能和上位阶的法的规范相抵触。宪法具有最高的法律效力，一切法律、法规都不得同宪法相抵触。法律的效力高于行政法规，行政法规不得同法律相抵触。法律、行政法规的效力高于地方性法规和规章，地方性法规和规章不得同法律、行政法规相抵触。地方性法规的效力高于地方政府规章，地方政府规章不得同地方性法规相抵触。

（2）我国信息安全法律体系

我国目前的信息化立法，尤其是信息安全立法，尚处于起步阶段，我国政府和法律界都清醒地意识到这一问题的重要性，正在积极推进这一方面的工作。我国政府现有的信息安全法律体系可以分为两个层次。一是法律层次，从国家宪法和其它部门法的高度对个人、法人和其它组织的涉及国家安全的信息活动的权利和义务进行规范。二是行政法规和部门规章层次。此外，我国很多地方也出台了直接针对信息安全的地方性法规和地方政府规章，丰富了我国信息安全法律体系的内容。但是，目前我国的信息立法也存在诸多问题，法律体系亟待完善。

（3）标准基础

本章从以下方面介绍了标准的基础知识：基本概念、标准的意义与作用、标准的层次与类别。重要的知识点有：强制性标准、自愿性标准、等同采用国际标准、国家标准、行业标准、地方标准、企业标准。

（4）我国信息安全标准化工作

我国政府高度重视信息安全标准化工作，在国家政策中对推进信息安全标准化工作做出了明确部署，专门成立了信息安全标准化工作组织机构，发布了“十一五”信息安全标准化工作规划，标准化工作取得了明显成果，标准的基础性、规范性作用进一步加强。

除了全国信息安全标准化技术委员会组织制定信息安全国家标准外，我国国家保密局负责管理、发布，并强制执行国家保密标准。国家保密标准适用于指导全国各行各业、各个单位国家秘密的保护工作，具有全国性指导作用，是国家信息安全标准的重要组成部分。我国还有一些行业标准化组织负责组织制定涉及信息安全的行业标准。这些行业标准化组织主要有公安部信息系统安全标准化技术委员会和中国通信标准化协会网络与信息安全技术工作委员会。我国信息安全国家标准的制定流程包括立项申请、工作组内征求意见、形成送审稿、秘书处网上征求意见、形成报批稿、安标委主任办公会审查、国标委批准发布、定期修订复审等阶段。

截至目前，全国信息安全标准化技术委员会共完成制定信息安全国家标准 76 项（13 项修订标准），有 50 项信息安全标准的研制在进行中。

（5）国外信息安全标准化组织及其工作进展

本章介绍了在信息安全标准领域有重要影响的一些国际和国外组织，重点是 ISO/IEC JTC1 SC27。该分委会主要从事信息技术安全的一般方法和技术的标准化工作。在 ISO 制定的信息安全国际标准中，评估标准具有基础性的地位。因此，本章还介绍了信息安全评估国际标准的发展情况，重点是 CC（通用准则）。最后，还介绍了 ISO/IEC JTC1 SC27 目前开展的各项标准制定工作的进展情况。

习题

1．我国法律分几个层次？
2．分析我国信息安全立法工作的现状。
3．概述强制性标准与自愿性标准的区别。
4．什么叫等同采用国际标准和等效采用国际标准？
5．我国的标准分几个层次？
6．我国有哪些涉及信息安全的标志化机构？

7．我国的信息安全国家标准制定流程是什么？
8．概述我国的信息安全标准体系。
9．列举至少三个国际或国外信息安全标准化组织。
10．概述国际信息安全评估标准的发展过程。

参考文献

1．Information Assurance Technical Framework (IATF), V3.1, NSA, September, 2003.

2．National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009. August 1997.

3．Defending America's Cyberspace National Plan for Information Systems Protection Version 1.0, the White House. January, 2000.

4．Department of Defense Global Information Grid Information Assurance, Department of Defense Chief Information Officer Guidance and Policy Memorandum No.6-8510. June 16, 2000.

5． ISO/IEC TR 13335-1：2000, Information Technology – Security Techniques . Guidelines for the Management of IT Security (GMITS). Part 1: Concepts and Models for IT Security. 1996.

6．ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation. August 1999.

7．NIST Special Publication 800-30. Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology. July 2002.

8．ISO/IEC 7498-1:1994, Information technology - Open Systems Interconnection - Basic reference model. November, 1994.

9．RFC 793: Transmission Control Protocol. Internet Engineering Task Force. September 1981.

10．RFC 791: Internet Protocol. Internet Engineering Task Force. October 15th, 1992

11．ISO 7498-2:1989. Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. January, 1989.

12．US Government, The Federal Information Security Management Act of 2002. October, 2002.

13．NIST Special Publication 800-41. Guidelines on Firewalls and Firewall Policy. National Institute of Standards and Technology. January 2002.

14．NIST Special Publication 800-31. Intrusion Detection Systems (IDS). National Institute of Standards and Technology. November, 2001.

15．NIST Special Publication 800-28. Guidelines on Active Content and Mobile Code. National Institute of Standards and Technology. October, 2001.

16．Douglas R. Stinson. Cryptography - Theory and Practice, 3rd Edition. Chapman&Hall/CRC, 2005.

17．A.Menezes, P.Oorshcot, and S.Vanstone. Handbook of Applied Crpytography. CRC Press, 1997.

18．Wenbo Mao. Modern Cryptography: Theory & Practice. Prentice Hall PTR, 2004.

19．N.Koblitz. A Course in Number Theory and Cryptography, 2nd Edition. Springer, 1994.

20．ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

21．US Federal Register. Vol. 72, No. 212. November 2, 2007.

22．Http://csrc.nist.gov/groups/ST/hash/sha-3/index.html.

23．Xiaoyun Wang, Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD, Crypto'04.

24．D.E.Bell and L.J.Lapadula, Secure Computer Systems: A Mathematical Model, MTR2547-II, AD 771543, The MITRE Corporation, Bedford, Massachusetts. May 1973.

25．D. E. Bell, Concerning "modeling" of computer security, in IEEE Symposium on Security and

Privacy. 1988.
26．Biba, K. J. "Integrity Considerations for Secure Computer Systems", MTR-3153, The Mitre Corporation, April 1977.
27．Stephen Tse, Steve Zdancewic: Run-time Principals in Information-flow Type Systems. IEEE Symposium on Security and Privacy 2004: 179-193.
28．Clark, David D.; and Wilson, David R.; A Comparison of Commercial and Military Computer Security Policies; in Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), Oakland, CA; IEEE Press, pp. 184–193. May 1987.
29．Dr. David F.C. Brewer and Dr. Michael J. Nash. The Chinese Wall Security Policy. 1989.
30．Ferraiolo, D.F. and Kuhn, D.R. Role-Based Access Control. 15th National Computer Security Conference. pp. 554-563. October 1992.
31．Sandhu, R., Coyne, E.J., Feinstein, H.L. and Youman, C.E. Role-Based Access Control Models". IEEE Computer (IEEE Press) 29 (2): 38–47. August 1996.
32．National Computer Security Center, Trusted Computer System Evaluation Criteria, 5200.28-STD. 1985.
33．National Computer Security Center, Trusted Network Interpretation of the TCSEC, NCSC-TG-005. 31 July 1987.
34．National Computer Security Center, Trusted Database Interpretation of the TCSEC, NCSC-TG-021. April 1991.
35．Avizienis A, Laprie J C, Randell B, et al. Basic concepts and taxonomy of dependable and secure computing. IEEE TransDependable Secur Comput, 2004, 1(1): 11—33.
36．Trusted Computing Group. TCG Specification Architecture Overview[EB/OL].[2007-08-02]. https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf.
37．Pearson S．Trusted Computing Platform，the Next Security Solution[R]．Bristol UK：HP Laboratories, 2002．
38．Smith S W, Palmer E R, et al. Using a High-performance, Programmable Secure Coprocessor. In Proceedings of the 2nd International Conference on Financial Cryptography, Anguilla, British West Indies, LNCS 1465, Springer-Verlag, 1998:73-89.
39．Smith S W, Austel V. Trusting Trusted Hardware: Towards a Formal Model for Programmable Secure Coprocessors. In Proceedings of the 3rd USENIX Workshop on Electronic Commerce, 1998.
40．Smith S W. Outbound Authentication for Programmable Secure Coprocessors. 7th European Symposium on Research in Computer Security, Zurich Switzerland, LNCS 2502, Springer-Verlag, 2002: 72-89.
41．Arbaugh W, Farber D J, et al. A Secure and Reliable Bootstrap Architecture. In Proceedings of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, USA, IEEE Computer Society, 1997: 65-71.
42．Trusted Computing Group TCG. http://www. Trustedcomputinggroup.org/.
43．Intel Corporation. LaGrande Technology ArchitecturalOverview. May 1, 2005. http://www.intel.com/technology/security．
44．Microsoft. Trusted Platform Module Services in Windows Longhorn．April 25, 2005. http://www..microsof.com/resources/ngscb/.
45．The Open Trusted Computing (OpenTC)consortium．General activities of OpenTC. January 1, 2006. http://www.opentc.net.

46．Trusted Computing Group. TCG TPM Specification Version 1.2 Revision 94, Design Principles. https://www.trustedcomputinggroup.org/specs/TPM/, 2006.
47．Trusted Computing Group. TCG TPM Specification Version 1.2 Revision 94, Structures of the TPM. https://www.trustedcomputinggroup.org/specs/TPM/, 2006.
48．Trusted Computing Group. TCG TPM Specification Version 1.2 Revision 94, Commands. https://www.trustedcomputinggroup.org/specs/TPM/, 2006.
49．Trusted Computing Group. TCG Software Stack Specification Version 1.2 Level1 ErrataA. July, 2007.
50．Systems Security Engineering Capability Maturity Model, Model Description Document, Version 2.0. April 1, 1999.
51．Systems Security Engineering Capability Maturity Model, Model Description Document, Version 3.0. June 3, 1999.
52．SSE-CMM Project, “SSE-CMM Appraisal Method,” Version 2.0, April 16,1999.
53．IAEC3186. Introduction to Information Systems Security Engineering (ISSE), Session 02-01. September 2001.
54．IEEE Standard for Application and Management of the Systems Engineering Process (IEEE Std 1220 1998).
55．ND186. Introduction to Information Systems Security Engineering (ISSE), Session 02-99, May 1999.
56．Information Systems Security Engineering Handbook, Release 1.0, 28 February 1994.
57．The Relationship Betwen the SSE-CMM and IT Security Guidance Documentation, John P. Hopkinson, EWA-Canada Ltd. 1999.
58．Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, John Wiley and Sons, ISBN 0-471-38922-6. 2001.
59．ISO/IEC TR 17799：2000 Information security Management —Code of Practice for Information Security Management.
60．ISO/IEC 27001:2005. Information technology - Security techniques - Information security management systems.
61．ISO/IEC 27002:2005. Information technology - Security techniques - Code of practice for information security management.
62．沈昌祥,左晓栋.非传统安全与现实中国丛书——信息安全.浙江大学出版社.2007 年 10 月.
63．中共中央办公厅 国务院办公厅关于印发《2006-2020 年国家信息化发展战略》的通知（中办发〔2006〕11 号）.
64．2008 年中国大陆地区电脑病毒疫情&互联网安全报告,2008 年 12 月 19 日.
65．第 23 次中国互联网络发展状况统计报告, 2009 年 1 月 13 日.
66．国家计算机网络应急技术处理协调中心 http://www.cert.org.cn.
67．沈昌祥,构造积极防御的安全保障框架[J].计算机安全,2003(32) :1-2.
68．Schneier B. 应用密码学——协议、算法与 C 源程序.吴世忠,祝世雄,张文正译.机械工业出版社, 2001.
69．信息安全原理与实践,(美) [M.斯坦普]Mark Stamp 著,杜瑞颖等译.电子工业出版社,2007.
70．赵战生,杜虹,吕述望等.信息安全保密教程,中国科学技术大学出版社.2006 年 4 月.
71．中华人民共和国电子签名法, 2004 年 8 月 28 日公布,2005 年 4 月 1 日起施行.
72．蔡谊,郑志蓉,沈昌祥.基于多级安全策略的二维标识模型.计算机学报,2004,27(5):619～624.

73．国家标准 GB 17859-1999 计算机信息系统安全保护等级划分准则.
74．闵应骅. 前进中的可信计算. 中国传媒科技,2005 年 9 月.
75．David Challener, Kent Yoder, Ryan Catherman 等.A pratical Guide to Trusted Computing.赵波,严飞,于发江等译.机械工业出版社,2008.
76．国家密码管理局,可信计算密码支撑平台功能与接口规范.2007 年 12 月 16 日. http://www.oscca.gov.cn/- UpFile/.
77．信息安全等级保护管理办法（公通字[2007]43 号）.
78．国家标准报批稿,信息安全技术 信息系统等级保护安全设计技术要求.
79．沈昌祥.信息安全工程导论,电子工业出版社.2003 年 7 月.
80．张红旗等,信息安全管理,人民邮电出版社.2007 年 11 月.
81．国家标准 GB/T 20984-2007 信息安全技术 信息安全风险评估规范.
82．国家标准 GB/T 22080-2008 信息技术安全技术 信息安全管理体系 要求.
83．国家标准 GB/T 22081-2008 信息技术 安全技术 信息安全管理实用规则.
84．中国信息安全认证中心 http://www.isccc.gov.cn.
85．国家标准 GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南
86．行业标准 YD/T 1799-2008 网络与信息安全应急处理服务资质评估方法
87．国家标准 GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
88．中华人民共和国立法法, 2000 年 3 月 15 日公布,2000 年 7 月 1 日施行.
89．中国国家标准化管理委员会 http://www.sac.gov.cn.
90．全国信息安全标准化技术委员会 http://www.tc260.org.cn.