高等学校电子信息学科“十二五”规划教材

信息安全工程与管理

唐成华　编著

西安电子科技大学出版社
http://www.xduph.com

高等学校电子信息学科“十二五”规划教材

信息安全工程与管理

唐成华　编著

西安电子科技大学出版社

内 容 简 介

本书以信息系统安全工程与管理的问题和要求为方向，以作者所在团队多年来在信息安全工程与管理方面相关教学以及研究工作为基础，参考最新的信息安全工程与管理相关标准和规范，提炼国内外信息安全工程与管理领域的最新成果，全面、系统地介绍了信息安全工程与管理的基本框架、体系结构、控制规范等相关知识。

本书主要内容包括：信息安全工程概述、ISSE 过程、SSE-CMM 工程、信息安全工程与等级保护、信息安全管理概述、信息安全管理控制规范、信息安全管理体系、信息安全风险评估和信息安全策略。

本书适用于高等院校信息安全专业、信息管理与信息系统专业、网络工程等专业本科及研究生教学，也可作为相关专业技术人员的参考书或培训教材。

图书在版编目(CIP)数据

信息安全工程与管理/唐成华编著. —西安：西安电子科技大学出版社，2013.1
高等学校电子信息学科“十二五”规划教材
ISBN 978-7-5606-2959-9

Ⅰ. ① 信… Ⅱ. ① 唐… Ⅲ. ① 信息安全—高等学校—教材 Ⅳ. ① TP309

中国版本图书馆 CIP 数据核字(2012)第 291466 号

策　　划　陈　婷
责任编辑　陈　婷　苗　娟
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西光大印务有限责任公司
版　　次　2012 年 12 月第 1 版　2012 年 12 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印　张　15.5
字　　数　365 千字
印　　数　1～3000 册
定　　价　27.00 元
ISBN 978-7-5606-2959-9/TP

XDUP 3251001-1

前　言

信息安全已经成为国家安全、社会安全和人民生活安全的重要组成部分。目前，我国信息安全防护能力处于发展的初级阶段，许多计算机还处于不设防状态。在核心技术、管理措施、防范意识等方面，与信息安全的实际需要存在很大的差距。由于信息安全的多层次、多因素和动态性等特点，从系统工程的角度来看，进行信息安全保障建设，并重视信息安全管理，是信息安全发展的必然趋势，且正在被社会各界所接受。近几年，信息安全工程与管理的相关模型、流程和方法发展迅速，相关的标准和法规也纷纷推出，整个信息安全工程与管理体系越来越完善。

信息安全工程要求对信息系统的各个环节进行综合考虑、规划和构架，遵循国内外相关信息安全标准与规范，考虑组织对信息安全各个层面上的实际需求，在风险分析的基础上引入适当的控制，建立合理的信息安全管理体系，以确保信息资产的保密性、完整性和可用性等。同时，要时时兼顾组织内外发生的变化，适时改进信息工程过程，不断完善信息安全管理体系。因此，实现信息安全是一个需要完整体系来保证的持续过程，这也是组织需要信息安全工程与管理的基本出发点。

信息安全保障建设离不开信息安全工程与管理，尤其是目前我国正在大力推进的等级保护工作，正是以工程化建设为主导思想，从相关法律法规和政策、相关标准体系、管理体系和技术体系等方面进行的全方位的信息安全建设。本书正是以此需求为出发点，在保证知识点讲解精炼的基础上，参考了最新的信息安全工程与管理相关标准和规范，并吸纳了国内外信息安全工程与管理理论和方法的最新成果，全书内容涉及信息安全工程与管理的方方面面。

全书共分 9 章，各章的内容既独立又有联系。第 1 章是信息安全工程概述；第 2 章、第 3 章分别介绍了信息安全工程 ISSE 的理论过程和信息安全工程能力成熟度模型 SSE-CMM；第 4 章详细阐述了我国基于等级保护制度的信息安全工程实施原理、方法及过程；第 5 章是信息安全管理的相关概述；第 6 章详细描述了信息安全管理的控制规范；第 7 章分析了信息安全管理体系的模型过程；第 8 章和第 9 章分别讨论了信息安全风险评估方法以及信息安全策略的制定过程与要求。

本书可以作为信息安全专业、信息管理与信息系统专业、网络工程等专业本科生及研究生教材，还可以供相关专业技术人员参考。

在编写过程中，笔者除引用了自己的一些研究内容和成果之外，还参考了大量国内外优秀论文、书籍，以及众多的信息安全工程与管理相关的标准和规范等。在此对这些资料的作者或编著机构表示由衷的感谢。另外，本书得到了中国电子教育学会“十二五”高等

教育科学研究立项课题(No.ZDJ11208)、新世纪广西高等教育教学改革工程立项项目(No.2012JGA137)、广西教育厅科研资助项目(No.201012MS088)、广西可信软件重点实验室开放基金项目(No.kx201111)的资助。

信息安全工程与管理是信息安全相关理论与技术的实践，是信息安全应用发展的趋势，本书对此领域的理论和方法进行了初步归纳，以期有益于读者。由于作者水平有限，书中疏漏与错误在所难免，恳请广大同行和读者批评指正。

编　者

2012 年 5 月

目　录

第1章 信息安全工程

1.1 信息安全的概念

1948年，美国贝尔实验室数学研究员、信息论的奠基人克劳德·香农(Claude Elwood Shannon，1916—2001)，在题为《通信的数学理论》的一篇论文中，给出了信息的数学定义，认为“信息是能够用来消除随机不确定性的东西”。同年，美国著名数学家、控制论的创始人诺伯特·维纳(Norbert Wiener，1894—1964)在《控制论》一书中指出，“信息就是信息，既非物质，也非能量”。

信息的实质是通过信号、指令等实现对物质和能量的调节与控制。

在当今社会，信息已成为与物质、能源同样重要的国家主要财富和重要战略资源，对信息优势的夺取，是衡量一个国家综合实力的重要参数，对信息的开发、利用和控制也已经成为国家利益争夺的重要目标。而对信息优势的夺取，直接表现为信息安全与对抗。能否有效地保护好已有的信息资源并争夺更优势的信息资源，保证信息化进程健康、有序、可持续发展，直接关乎国家安危、民族兴亡。因此，信息安全已成为国家安全、社会安全和人民生活安全的重要组成部分。

1.1.1 信息安全的基本范畴

信息安全的基本范畴，包括信息资源、信息价值、信息作用、信息损失、信息载体、信息环境等。

信息资源，即信息的资源化或资源化的信息，是经过主观处理或加工，能够传输或传播，可对社会生活发挥作用的信息总和。按照该作用的促进方向，信息资源可分为有价值信息和中性信息。

信息价值，是信息资源优势的反映，可分为积极价值和消极价值。信息安全的基本范畴是建立在信息资源优势改变或信息价值损失的基础上的，即信息作用以对信息价值的影响来衡量，信息损失以信息价值的损失为量度。

信息作用，是指信息资源在实现信息价值过程中，所发生的对周围环境或自身的影响或改变。这些影响或改变，与人的主观意愿无关，但可以为人的主观意愿服务，可以被敌我双方利用，实现积极作用或消极作用。

信息损失，是指信息价值的损失，是在消极信息作用影响下的信息资源的价值降低的量度。信息损失是信息安全范畴里的重要负面计算指标，以定量、定性或概率的方式来评估主体活动与信息安全的影响与程度。

信息载体，是指信息在传输或传播中携带信息的媒介，即用于记录、传输和保存信息的软、硬件实体，包括以能源和介质为特征，运用声、光、电等传递信息的无形载体和以实物形态记录为特征，运用纸张、胶片、磁带或磁盘等传递和贮存信息的有形载体。

信息环境，是与信息活动有关的外部环境的集合，包括机房、电力、温度、湿度、防火、防水、防震、防辐射等硬环境，也包括国家法律法规、部门规章、政治经济、社会文化、教育培训、人员素质、监督管理等软环境。

1.1.2 信息安全工程的概念

信息安全工程研究如何建立能够面对错误、攻击和灾难的可靠信息系统。

许多信息系统都有严格的安全保障要求，否则，一旦发生安全问题和处理不当，会产生严重的甚至灾难性的后果。例如，核安全控制系统失败，会危及人类生存和环境；航空安全系统失败，会严重影响机组安全；ATM 银行系统失败，会破坏经济生活秩序；股票交易系统失败，会损害用户权利；网上支付系统失败，会阻碍网络经济的发展；财务报账系统失败，会扰乱经费管理体系。

一般认为，软件工程是要保证某些事情能够发生(如“能提供 pdf 格式文档的报表输出功能”)，而安全工程是要确保某些事情不能发生(如“要提供 pdf 格式文档的防拷贝功能”)。不同的系统工程建设与不同的设计目标和要求有关，而其中安全工程的建设尤其复杂。对于信息安全工程，需要考虑到特定信息系统的安全保护需求、可能存在的安全隐患以及相应的解决方法等。

为了更好地理解信息系统安全工程的需求、隐患、方法，及其工程化概念，首先来了解以下三个领域的信息系统实例：银行、机场、家庭。

例一：银行

因为业务的需要，银行需要运行大量的对安全要求很苛刻的计算机系统。

银行信息系统包括银行综合业务系统、银行渠道系统、网上银行系统、跨行支持系统、中国银联支持系统等。在中国，通过中国国家金融通信网络(CNFN，China National Financial Network)将中央银行、各商业银行和其他金融机构连接在一起，构成全国性的金融专用网络系统。

(1) 银行业务的核心是记账系统。它保存客户的主账目信息和记录每日业务的分类账目。由于该系统一般由银行员工进行操作，要求遵守相应的法律、规章制度和操作程序等，因此，对该系统的威胁主要来自银行内部员工利用职务便利和系统漏洞进行的违法犯罪行为。例如，冒用客户身份的信用卡诈骗、伪造并使用伪造的银行票据等；当然也包括银行员工无意的操作失误、违反规定的越权操作行为，如每次借贷记录的正负数字不匹配、大额转账的私自认可等。所以，对于银行记账系统，要求有账户及操作权限控制策略、异常交易监控及报警系统、严格的银行内部网络访问控制规章制度等。

(2) 银行 ATM 机是安全与方便的“博弈”。不管是在行式，还是离行式，ATM 机都大大方便了客户自行进行账户资金的处理，但同时也经常出现漏洞和异常，例如，账户信息被偷窃、异常吞卡或吐钞、网络故障造成的服务异常中断、网络通信中的信息泄露等。因此，这就要求有高强度的 ATM 与银行的通讯信息加密系统、客户身份认证系统、服务异常

的应急响应系统、客户行为记录与取证系统等的安全支持。

(3) 大部分银行都有保险箱的金融保障服务，但也存在一些突出的安全问题，如在硬件老化、设备配置不足、软硬件功能存在缺陷的情况下，可能诱发内部员工作案的动机或使外部盗窃有机可乘，导致客户财物失窃、毁损，同时银行还可能面临商业信誉下降、客户提出巨额赔偿等。因此，应该整体规划，优化保险箱系统，加强报警系统安全防护能力，加密监控信息防伪造功能，增加系统稽核功能和预警功能，提高安保人员素质，增加异地监控等。

(4) 由于技术发展和扩展业务的需要，目前“网上银行”发展迅速，客户足不出户就能够便捷地管理存款、支票、信用卡及进行个人投资等非现金交易。网上银行使银行内部网络向互联网敞开了大门。网上银行系统的安全关系到银行内部整个金融网络的安全，应当防止黑客攻击网络修改记账系统，要求设立防火墙来隔离相关网络，采用高安全级的 Web 应用服务器，24 小时实时安全监控，进行有身份识别的 CA 认证，实施网络通讯的安全加密，进行用户证书的安全管理和网络银行个人认证介质的管理等。

例二：机场

当地时间 2011 年 1 月 24 日 16 时 32 分，俄罗斯莫斯科多莫杰多沃机场抵达大厅内发生自杀式炸弹爆炸，造成 35 人死亡，130 余人受伤。而据美国合众国际社报道，美国政府 2011 年 7 月 13 日发布的两篇报告中显示，过去 10 年间，美国机场共出现超过 25 000 个安全漏洞。

(1) 安检与旅客隐私的冲突。很多安全漏洞是安检时没有执行系统扫描或扫描错误等造成的。采用“全身扫描安检技术”，如果使用得当，可以提高机场的安检水平，但同时该技术会显露旅客的身体轮廓，过于侵犯个人隐私。因此，人们都在期待第二代“人体扫描仪”，该信息检测系统平时只显示黑屏，只在发现可疑物品时才发出警报并显示可疑部位，另外，扩大安全半径，例如以色列在通往特拉维夫本-古里安国际机场的主要道路上就开始设置安检站，使安检系统真正发挥作用，而不成为摆设，从制度和技术上建立一套“综合检查机制”。

(2) 航空指挥系统是保证航空安全的重要技术手段。航空运输时间紧、任务急、航线多、部门多、层次多，需要建立各级指挥职能系统，同时，在指挥调度室内按指挥区域可分为航行指挥、客机坪现场指挥，以及各有关业务部门的调度室或值机组，这些不同层次和级别的指挥系统间的信息传输与执行，要求信息的准确性、保密性和实时性，这涉及到信息系统的通信协议安全技术、数字加密技术、数字签名与认证技术、数据优化技术等。

(3) 航班信息管理与显示系统是机场保障旅客正常流程的重要环节，是机场直接面向旅客提供公众服务的重要手段，同时又是机场与旅客进行沟通的窗口，主要以多种显示设备为载体，显示面向公众发布的航班信息、公告信息、服务信息等，为旅客、楼内工作人员和航空公司地面代理提供及时、准确、友好的信息服务。因此，对航班数据的准确性提出了较高的要求，要求有实时动态数据的防篡改功能，同时对众多显示设备运行状况要进行严格监控，要有设备监测与故障诊断能力，保证系统的高效、稳定和安全运行。

例三：家庭

现在，越来越多的普通家庭都应用了广泛的分布式信息系统服务。

(1) 家庭可以通过电子商务系统进行网上购物，通过网上银行进行水、电、气、电话

等费用的在线支付。另外，很多家庭使用了汽车 GPS 系统、汽车遥控防盗系统、通过手机的汽车控制信息系统、卫星及数字电视接收系统等。只要使用了这些系统，安全问题就会随之而来，诸如网上诈骗、支付失败、遥控信息被劫持、系统链接数据异常等都能带来损失或伤害。因此，需要采用严格的网络信息存储、传送、加密、认证等方法，同时要求用户进行正确的操作，并完善相应的法律法规，来规避或约束这些威胁风险。

(2) 许多家庭开始使用家庭理财管理信息系统，统计家庭的房产、家居、电器等实物财产，统计家庭每月的薪资、租金等现金或银行存款收入，以及统计家庭的还贷、保险、教育、疾病、水、电、气、电话、手机、交通、汽油、食用油、米、菜、盐、牛奶、水果等支出，由此来培养珍惜自己劳动的好习惯，享受积累财富的乐趣。家庭理财管理信息系统甚至可以与网上消费系统进行无缝链接，因此，在使用家庭理财管理信息系统时，除了自身的家庭信息安全之外，还要考虑这些信息暴露在互联网上时的数据保密性、完整性和可控性等要求。

(3) 智能家居控制系统可担当家庭的信息家电控制中心的角色，把诸如电视机、空调、热水器、室内监控器、VCD(DVD、录像机)、功放等多种家用电器的控制功能分门别类地储存起来，在需要的时候随时调用，实现了多种家电在相同或不同时间段的自动运行，极大地提升了生活质量。这种数字化家庭信息系统是一个智能家庭综合监、控、管平台，对整合的各个相关设备的信息处理要求有较高的保密性、准确性和可控性等。在数据统一协调过程中容易受到攻击是系统的弱点，要避免设备运行或联动时产生失败、紊乱、被劫持等后果。

从以上实例可以看出，各领域的信息系统安全与安全需求、安全隐患、解决方法紧密相关。解决信息安全问题，不能简单地依靠纯粹的技术，也不是安全产品的堆砌，而是要依赖于复杂的信息安全系统工程。

在工程上，信息安全是与风险相联系的概念，通过风险管理与控制来实现。信息安全风险是信息价值、系统脆弱性和系统威胁等三个变量的函数，如图 1-1 所示。

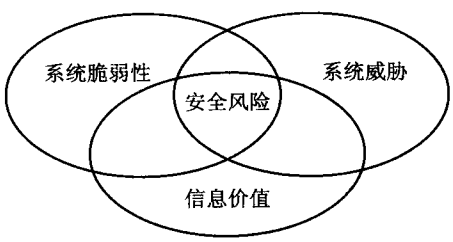

图 1-1　信息安全风险

系统脆弱性是指可以被用来获取、利用、损坏、颠覆信息资源的方式。系统威胁是指利用系统脆弱性，可能造成某个有害结果的事件或对系统造成危害的潜在事实。而安全风险就是某种威胁利用系统脆弱性对组织或机构的信息价值造成损失的潜在的可能性。信息安全风险管理与控制是一个信息风险的测量、识别、控制及其最小化的过程，即在给定的信息损失约束下，协调信息价值、系统脆弱性和系统威胁之间关系的过程。

信息安全工程是采用系统工程的概念、原理、技术和方法，来研究、设计、开发、实施、管理、维护和评估信息系统安全的过程，是将经过时间考验证明是正确的工程实践流程、管理技术和当前能够得到的最好的技术方法相结合的过程。

目前信息安全工程存在于广泛的信息系统的应用中。对于任何一个应用，考虑和确定安全需求、找出安全隐患或系统脆弱性、制定并执行面对系统威胁的安全策略、评估其所承受的安全风险等，都是很有必要的。信息安全工程正在变成一个日益重要的学科，它不仅用于信息系统和应用程序的设计、开发、集成、操作、管理、维护和评估，也适用于企业和商业信息产品的开发、发布和评估。因此，信息安全工程可应用于一个信息系统、一个信息产品或者一种信息服务中。

1.2　信息安全保障体系

1.2.1　信息保障是信息安全的新发展

信息安全问题始终伴随着信息技术的发展而发展，先后经历了“通信保密”(COMSEC)、“信息系统安全”(INFOSEC)和目前的“信息保障”(IA)三个阶段。每个阶段虽然在满足的需求、关注的目标以及发展的技术等方面各不相同，但其根本出发点都是要保护信息，确保其能为己所用。

20 世纪 40～70 年代，信息安全以通信保密为主体，要求实现信息的保密性，其时代标志有 1949 年香农发表的《保密系统的信息理论》、1976 年由 Diffie 与 Hellman 在“New Directions in Cryptography”一文中提出的公钥密码体制、1977 年美国国家标准局(NBS，National Bureau of Standards，NIST 的前身)公布的数据加密标准(DES)。这一时期的信息安全所面临的主要威胁是搭线窃听和密码学分析，信息安全需求基本来自军政指挥体系方面的“通信保密”要求，主要目的是使信息即使在被截获的情况下也无法被敌人使用，因此其技术主要体现在加密和解密设备上。

20 世纪 70～80 年代，随着小规模计算机组成的简单网络系统的出现，网络中多点传输、处理以及存储的保密性、完整性、可用性问题成为关注的焦点，其时代标志是 1985 年美国国防部(DOD，United States Department of Defense)公布的《可信计算机系统评估准则》(TCSEC，Trusted Computer System Evaluation Criteria)将操作系统的安全级别分为 4 类 7 个级别。这一时期的主要安全威胁扩展到非法访问、恶意代码、脆弱口令等方面，计算机之间的信息交互，要求人们必须在信息存储、处理、传输过程中采取措施，保护信息和信息系统不被非法访问或修改，同时不能拒绝合法用户的服务请求，其技术发展主要体现在访问控制上。这时，人们开始将“通信安全”与“计算机安全”合并考虑，“信息系统安全”成为研究热点。

进入 20 世纪 90 年代，随着网络技术的进一步发展，超大型网络迫使人们必须从整体安全的角度去考虑信息安全问题。网络的开放性、广域性等特征把人们对信息安全的需求，延展到可用性、完整性、真实性、保密性和不可否认性等更全面的范畴。同时，随着网络黑客、病毒等技术层出不穷、变化多端，人们发现任何信息安全技术和手段都存在弱点，传统的“防火墙+补丁”这样的纯技术方案已无法完全抵御来自各方的威胁，必须寻找一种可持续的保护机制，对信息和信息系统进行全方位的、动态的保护。1995 年，美国国防部发现其计算机网络系统遭受了 725 万余次的外来袭击。当时国防部认为，其计算机系统防

御能力相当低下，对袭击的发现概率仅为 12%，能做出反应的还不到 1%，这种紧迫形势引起了美军方的高度重视。1996 年 11 月，美国国防部国防科学委员会(DSB，Defense Science Board)的一份关于信息战防御能力的评估报告再次指出，国防部网络、信息系统存在很多漏洞和薄弱环节，而且未来还会面临更加严峻的挑战，要求国防部必须采取特别行动来提高国防部应对现有和不断出现的威胁的能力。为此，1996 年在美国国防部令 S-3600.1 中首次给出了“信息安全保障”的概念，即“保护和防御信息及信息系统，确保其可用性、完整性、保密性、可追究性、抗否认性等特性。这包括在信息系统中融入保护、检测、响应功能，并提供信息系统的恢复功能”，并在《联合设想 2010》中，正式把“信息保障”确定为信息优势能力的重要组成，在此指导之下，提出了“信息保障战略计划”，旨在构建一种动态、可持续、全方位的信息保障机制。从 1998 年开始，美国国家安全局(NSA，National Security Agency)在《信息保障技术框架》(IATF)中不断完善其“深度防御”(Defense-in-Depth)的核心战略，并在 2002 年 9 月将 IATF 更新为 3.1 版本。

1.2.2　信息保障的构成及其空间特性

信息保障强调信息安全的保护能力，同时重视提高系统的入侵检测能力、事件响应能力和快速恢复能力，它关注的是信息系统整个生命周期的保护、检测、响应和恢复等安全机制，即 PDRR(Protection/Detection/Response/Recovery)安全模型，其构成如图 1-2 所示。

图 1-2　信息保障的构成

就本质而言，信息保障是一种确保信息和信息系统能够安全运行的防护性行为，是信息安全在当前信息时代的新发展。信息保障的对象是信息以及处理、管理、存储、传输信息的信息系统，目的是采取技术、管理等综合性手段，使信息和信息系统具备保密性、完整性、可用性、可认证性、不可否认性，以及在遭受攻击后的可恢复性。与以前的信息安全概念相比，信息保障概念的范围更加广泛。从理念上看，以前信息安全强调的是“规避风险”，即防止发生破坏并提供保护，但破坏发生时无法挽回；而信息保障强调的是“风险管理”，即综合运用保护，检测、响应和恢复等多种措施，使得信息在攻击突破某层防御后，仍能确保一定级别的可用性、完整性、真实性、保密性和不可否认性，并能及时对破坏进行修复。再者，以前的信息安全通常是单一或多种技术手段的简单累加，而信息保障则是对加密、访问控制、防火墙、安全路由等技术的综合运用，更注重入侵检测和灾难恢复等技术。

信息安全保障“深度防御”的基本思想就是要对攻击者和目标之间的信息环境进行分层，然后在每一层都“搭建”由技术手段和管理策略等综合措施构成的一道道“屏障”，形

成连续的、层次化的多重防御机制，保障用户信息及信息系统的安全，消除给攻击网络的企图提供的“缺口”。深度防御的空间特性如图 1-3 所示。

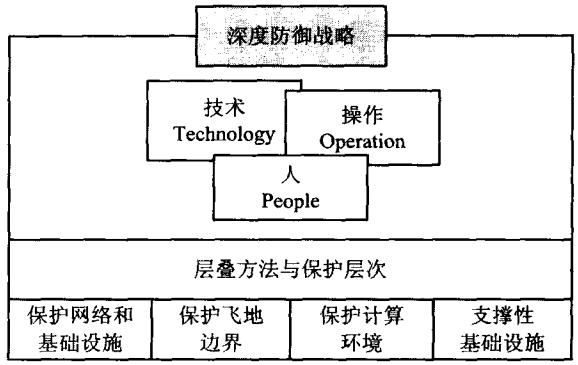

图 1-3　深度防御的信息保障战略

深度防御的信息保障战略强调人、技术和操作三个核心的原则，对技术和信息基础设施的管理也离不开这三个要素。

(1) 人(People)：人是信息体系的主体，是信息系统的拥有者、管理者和使用者，是信息保障体系的核心，是第一位的要素，同时也是最脆弱的要素。正因为如此，关于人的安全管理在安全保障体系中非常重要，可以说，信息安全保障体系，实质上就是一个安全管理的体系，其中包括意识培训、组织管理、技术管理和操作管理等多个方面。技术是安全的基础，管理是安全的灵魂，所以应当在重视安全技术应用的同时，必须加强安全管理。

(2) 技术(Technology)：技术是实现信息保障的重要手段，信息保障体系所应具备的各项安全服务就是通过技术机制来实现的。当然，这里所说的技术，已经不单是以防护为主的静态技术体系，而是关于防护、检测、响应和恢复并重的动态技术体系。

(3) 操作(Operation)：或者叫运行，它构成了安全保障的主动防御体系，如果说技术的构成是被动的，那么操作及其流程就是将各方面技术紧密结合在一起的主动的过程，其中包括风险评估、安全监控、安全审计、跟踪告警、入侵检测、响应恢复等内容。

“深度防御”的信息保障战略将安全空间划分为 4 个纵深防御焦点域：保护网络和基础设施、保护飞地边界、保护计算环境以及支撑性基础设施。基于“深度防御”的信息保障战略的空间特性来建设信息安全保障体系，需要解决支撑性基础设施、内部网络、网络边界、网络通信基础设施和主机计算等环境的安全防御问题，其技术准则的分析模型如图 1-4 所示。

(1) 网络及其基础设施是各种信息系统的中枢，为用户信息存储与获取提供了一个传输机制，它的安全是整个信息系统安全的基础。网络和基础设施的防御包括维护信息服务、防止拒绝服务攻击(DoS)、保护数据流分析和在整个广域网上交换的公共的、私人的或保密的信息，并避免这些信息在无意中泄漏给未授权访问者或发生更改、延时、发送失败等。

(2) 根据业务的重要性及管理等级和安全等级的不同，一个信息系统通常可以划分为多个飞地，每个飞地是在单一安全机制控制下的物理区域环境，具有逻辑和物理的安全措施。这些飞地大多具有和其他区域或网络相连接的外部连接。飞地边界防御关注的是如何对进出飞地边界的数据流进行有效的控制与监视，例如在飞地边界安装防火墙、隔离器等基础设施来实施保护。

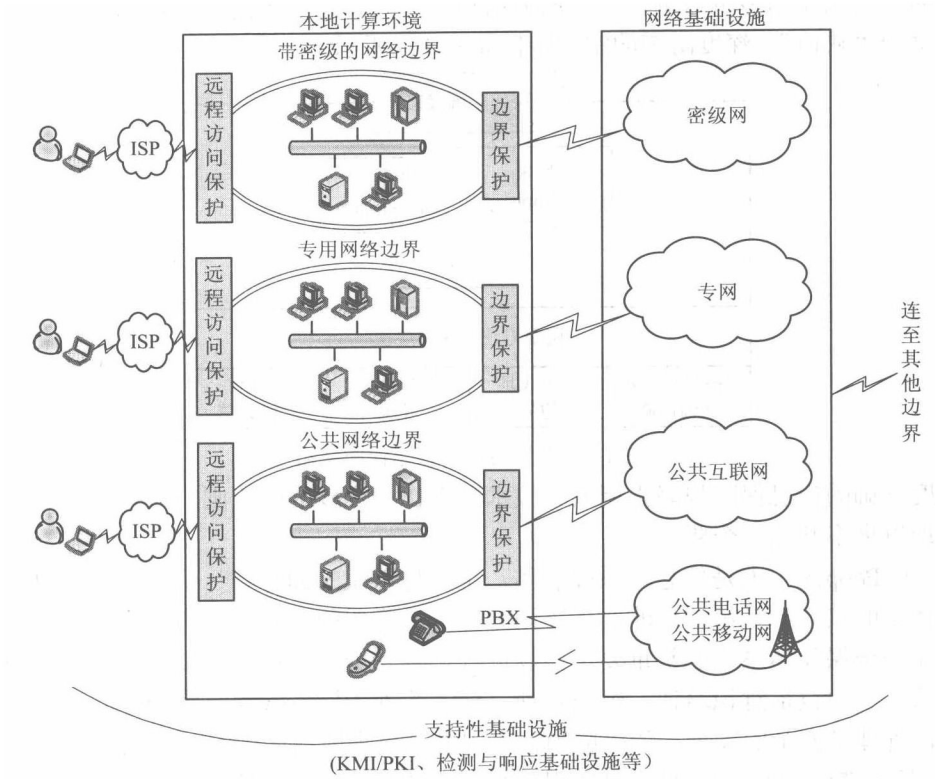

图 1-4　信息保障空间技术准则分析模型

(3) 在计算环境中的安全防护对象包括用户应用环境中的服务器、客户机以及所安装的操作系统和应用系统，这些应用能够提供包括信息访问、存储、传输、录入等服务。计算环境防御就是要利用识别与认证(I&A)、访问控制、VPN 等技术确保进出内部系统数据的保密性、完整性和不可否认性。这些是信息系统安全保护的最后一道防线。

(4) 支撑性基础设施是一套相关联的活动与能够提供安全服务的基础设施相结合的综合体。目前深度防御策略定义了两种支撑性基础设施：密钥管理基础设施(KMI)/公钥基础设施(PKI)、检测与响应基础设施。KMI/PKI 涉及网络环境的各个环节，是密码服务的基础，其中本地 KMI/PKI 提供本地授权，广域网 KMI/PKI 提供证书、目录以及密钥产生和发布功能。检测与响应基础设施则提供用户预警、检测、识别可能的网络攻击、做出有效响应以及对攻击行为进行调查分析等功能。

1.2.3　信息安全保障模型

信息安全保障模型如图 1-5 所示。

为了实现信息安全保障，首先要在信息域对网络空间进行数据获取、收集、保护、协同处理等，同时基于该过程取得相对于攻击者的信息有利地位，建立具有信息优势的能力，并为认知域所感知。其次，作为同步与响应，要在认知域进行推理和决策，在相关法律法规及标准指导下，建立产生和共享高质量的风险管理与控制、态势感知、理解、评估、预测等能力，并且基于风险和态势实现防御过程的实时自我调整过程。