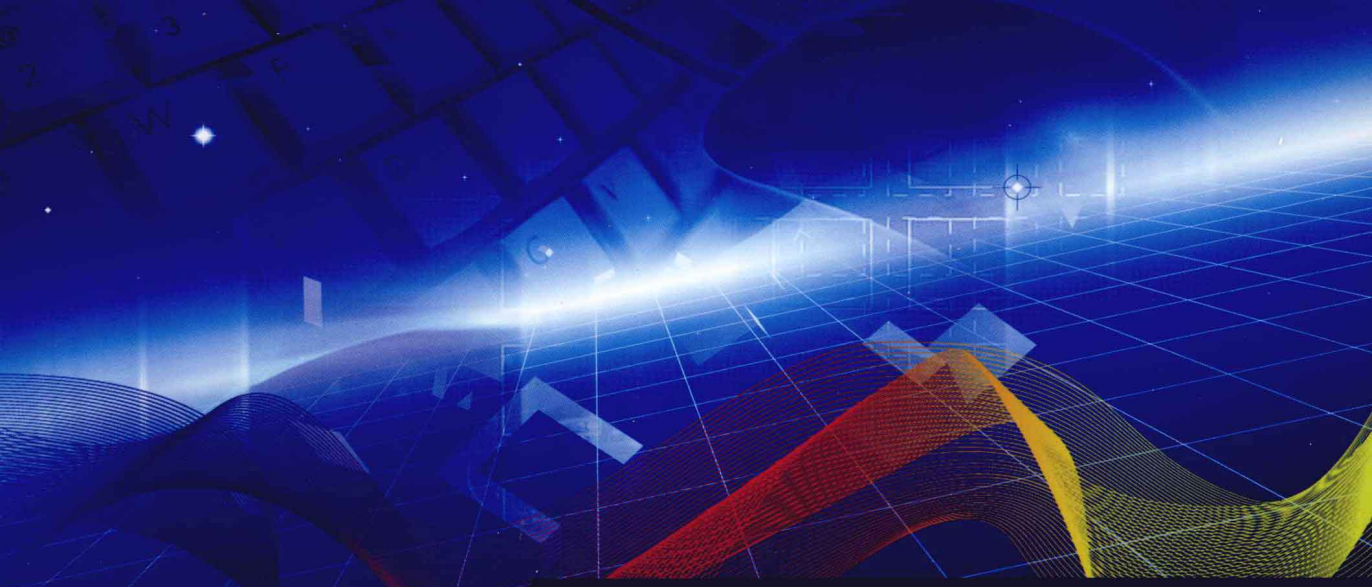

信息安全体系结构

张建标 赖英旭 侍伟敏◎编著

XINXI ANQUAN TIXI JIEGOU

北京工业大学出版社

信息安全体系结构

张建标　赖英旭　侍伟敏　编著

北京工业大学出版社

内 容 简 介

本书围绕信息安全体系结构设计，系统介绍了信息安全的基本知识、概念和原理。全书共分8章，主要内容包括信息安全体系结构的概念、设计框架和设计原则，并从物理安全、系统安全、网络安全和应用安全等方面介绍了各层次的设计要求和关键技术，最后介绍了信息安全管理和安全评估标准。本书内容丰富、概念清晰、系统性强、重点突出。

本书适合作为高等院校信息安全专业、计算机和通信等相关专业的本科生和研究生教材，也可供从事信息安全教学、科研和工程技术的相关人员参考。

图书在版编目（CIP）数据

信息安全体系结构/张建标，赖英旭，侍伟敏编著．
—北京：北京工业大学出版社，2011.8
ISBN 978-7-5639-2809-5

Ⅰ.①信… Ⅱ.①张… ②赖… ③侍… Ⅲ.①信息系统-安全技术 Ⅳ.①TP309

中国版本图书馆CIP数据核字（2011）第163608号

信息安全体系结构

编　　著：张建标　赖英旭　侍伟敏
责任编辑：董志乔
出版发行：北京工业大学出版社
（北京市朝阳区平乐园100号　100124）
010-67391722（传真）bgdcbs@sina.com
出 版 人：郝　勇
经销单位：全国各地新华书店
承印单位：徐水宏远印刷有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：13.75
字　　数：335千字
版　　次：2011年9月第1版
印　　次：2011年9月第1次印刷
标准书号：ISBN 978-7-5639-2809-5
定　　价：25.00元

前　言

随着信息技术的飞速发展和我国信息化进程的不断推进，各种基础信息网络和重要信息系统已经成为国家关键基础设施，支撑着网络通信、电子商务、电子政务、电子金融等各方面的应用。国民经济和社会发展对信息化的高度依赖，信息安全事件的不断增多，使信息安全问题日渐突出。信息安全问题直接影响到社会经济、政治、军事、个人生活等各个领域，甚至影响到国家安全。

面对不断出现的信息安全事件，规划、设计和建设安全的网络信息系统已非常重要。本书从信息安全体系结构角度出发，阐述了安全体系结构的规划设计、各个层次需要采用的关键技术和产品等问题。另外，也包括了信息安全管理、等级保护和安全评估等内容。

本书分为8章。第1章概述，介绍了信息安全的概念和我国的主要信息安全政策；第2章信息安全体系结构设计，介绍了几种典型的信息安全体系结构，以及信息安全的需求分析、设计目标和设计原则；第3章物理安全，介绍了物理安全中的环境安全、电源系统安全、设计安全和通信线路安全；第4章系统安全，介绍了系统硬件平台安全、操作系统安全、数据库安全、系统安全监测和备份与恢复；第5章网络安全，介绍了防火墙、入侵检测、VPN、漏洞扫描和网络安全集成等关键技术和产品；第6章应用安全，介绍了应用安全基础设施、Web安全、电子邮件安全和电子商务安全；第7章信息安全管理，介绍了ISO 27000系列国际标准，并对ISO 27001和27002两个主要标准进行了详细介绍；第8章安全评估标准，介绍了可信计算机系统评估准则、通用评估准则和计算机信息系统安全保护等级划分准则。

本书内容丰富、概念清晰、系统性强、重点突出。每章的小结对该章的重点内容进行了简要概括；各章后均附有习题，用于强化重要概念，测验读者对基本概念、重要内容的理解和掌握程度。

张建标拟定本书的编写内容和大纲，并编写第1、2、7、8章；赖英旭编写第3、5章；侍伟敏编写第4、6章。本书在编写过程中参考了国内外许多文献和书籍，并从中得到启发，在此一并表示感谢。

由于作者水平有限，书中内容难免有不当或错误之处，恳请专家和广大读者批评指正。

编　者

目　录

第1章 概 述

随着信息技术的飞速发展和我国信息化进程的不断推进，各种基础信息网络和重要信息系统已经成为国家的关键基础设施，支撑着网络通信、电子商务、电子政务、电子金融等各方面的应用。国民经济和社会发展对信息化的高度依赖，信息安全事件的不断增多，使信息安全问题日渐突出。信息安全问题直接影响到社会经济、政治、军事、个人生活等各个领域，甚至影响到国家安全。不解决信息安全问题，不加强基础信息网络和重要信息系统的安全保障，信息化不可能得到持续健康的发展。

2003年中共中央办公厅、国务院办公厅发布的《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）指出，“随着世界科学技术的迅猛发展和信息技术的广泛应用，特别是我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性、全局性作用日益增强，信息安全已经成为国家安全的重要组成部分”。2004年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”。

在信息化过程中，信息安全问题越来越多，确保信息安全越来越重要；但信息安全不是最终目的，只是服务于信息化的一种手段，其主要目的是为信息化保驾护航。

1.1 信息安全

人类社会经历了农业社会和工业社会后，已发展到当今的信息社会。2006年3月举行的第60届联合国大会已确定每年的5月17日为“世界信息社会日”，这标志着信息化对人类社会的影响进入了一个新的阶段。加快信息化发展，使信息化向纵深推进，推动信息社会建设已经成为世界各国的共同选择。在农业社会和工业社会中，物质和能源是主要资源，人们所从事的是大规模的物质生产。而在信息社会中，信息成为比物质和能源更为重要的资源，以开发和利用信息资源为目的的信息经济活动迅速扩大，逐渐取代工业生产活动而成为国民经济活动的主要内容。信息资源已经成为信息社会中不可或缺的基本生活要素，信息化要求最大限度地有效利用信息资源，从而推动社会全面进步。

在信息社会，信息是重要资源，也是无形财富。那么，什么是信息呢？信息反映的是一切物质和事物的属性，因此，可以说信息是客观事物通过物质载体所发出的消息、情报、指令、数据、信号中所包含的一切可传递和可交换的知识内容。信息必须通过一定载体才能得

以体现、存储和传播，这些载体可以是语言、文字、图像等。但是信息不会因为载体的不同而改变他所反映的事物的本质。什么是安全呢？在现代汉语词典中，“安全”的含义是指“没有危险；不受威胁；不出事故”。因此，信息安全笼统地讲，即是指信息这种资源在使用过程中应没有危险，不会受到威胁。如何更深入地理解信息安全这个概念呢？信息安全的概念与信息的本质属性密切相关，他是信息的本质属性所体现的安全意义。经过长期的探索和总结，人们归纳出了信息的三大基本安全属性。

1.1.1 信息的安全属性

1. 保密性（confidentiality）

保密性是指信息不能被未授权的个人、实体或者过程利用或知悉的特性。保证保密性的方法主要包括：

① 物理保密。采用各种物理方法，如限制、隔离、控制等措施保护信息不被泄露。

② 信息加密。采用密码技术加密信息，没有密钥的用户无法解密密文信息。

③ 信息隐藏。将信息嵌入其他客体中，隐藏信息的存在。

④ 电磁屏蔽。防止信息以电磁的方式（电磁辐射、电磁泄漏）发送出去。

保密性不仅包括信息内容的保密，而且包括信息状态的保密。

2. 完整性（integrity）

完整性是指数据没有遭受以非授权方式所作的篡改或破坏。影响信息完整性的主要因素有：设备故障，传输、处理和存储过程中产生的误码，人为攻击和计算机病毒等。保证完整性的方法主要包括：

① 协议。通过安全协议自身检测出被丢失、重复和乱序的信息，重放的信息，修改的信息。

② 检错、纠错编码方法。完成检错和纠错功能，常用的奇偶校验就是检错编码。

③ 密码校验和方法。实现抗篡改和验证传输是否出错。

④ 数字签名。保证信息的真实性，说明其未受到篡改。

⑤ 公证。通过第三方公证机构证明信息的真实性。

保密性要求信息不被泄露给未授权的人，而完整性要求信息不致受到非授权的篡改或破坏。

3. 可用性（availability）

可用性是指根据授权实体的要求可被访问和可被使用的特性。网络环境下的可用性不仅包括用户可访问硬件和软件资源，而且包括用户有能力获得所期望的服务质量，如具有一定吞吐量的网络带宽。

保证可用性的最有效方法就是提供一个具有普适安全服务的网络环境。通过访问控制阻止资源的未授权访问，利用保密性和完整性服务避免数据被泄露或被修改，另该网络环境能防止针对可用性的攻击，如 DDoS（分布式拒绝服务）攻击等。保证可用性的方法主要包括

以下几种。

① 避免遭受攻击。一些基于网络的攻击旨在破坏、降低服务等级或摧毁网络资源。免受攻击的方法包括：关闭操作系统和网络配置中的安全漏洞、控制授权实体对资源的访问、限制监测流经系统的数据来防止插入病毒等有害数据、防止路由表等网络数据的泄露。

② 避免未授权使用。当资源被使用、占用或过载时，其可用性会受到限制。如果未授权用户占用了有限的资源，如处理能力、网络带宽等，那么授权用户就不可用了。避免未授权使用的方法包括：通过访问控制限制未授权用户使用资源。

③ 防止例程失败。正常的操作失误和自然行为也可能导致系统可用性降低。解决的方法包括：使用具有高可靠性的设备、提供设备冗余和提供多路径的网络连接。

上述3个基本安全属性在世界范围内已得到了各国专家的共识。但是，对于信息的其他安全属性，信息安全界还没有统一的意见。在我国强调较多的有信息的可控性和不可否认性。

4. 可控性（controllability）

可控性是指能够控制使用信息资源的人或实体的使用方式，可控性是信息安全的必然要求。社会中存在着不法分子和各种敌对势力，不加控制地广泛使用信息安全设施和装置时，会严重影响政府对社会的监控管理行为。另外，从国家层面看，信息安全中的可控性除了对信息的可控外，还包括对安全产品、安全市场、安全厂商和安全研发人员的可控。

5. 不可否认性（non-repudiation）

不可否认性也称抗抵赖性，它是传统社会的不可否认需求在信息社会中的延伸。传统社会中的公章、印戳、签名等手段是实现不可否认性的主要机制。保证不可否认性的技术主要包括数字签名、可信第三方和公证等。

1.1.2 信息安全的发展历程

随着社会和技术的进步，信息安全也经历了一个发展的过程。了解信息安全的发展历程，可以更加全面地理解信息安全的概念。普遍认为，信息安全的发展可以划分为3个阶段，即通信安全（COMSEC）阶段、计算机安全（COMPUSEC）和信息安全（INFOSEC）阶段、信息保障（IA）阶段。

1. 通信安全（COMSEC）阶段

通信安全阶段开始于20世纪40年代，其主要标志是1949年Shanon发表的《保密系统的通信理论》（Communication Theory of Secrecy Systems），该理论将密码学的研究纳入了科学的轨道。本阶段主要关注的对象是军方和政府，所面临的主要安全威胁是搭线窃听和密码学分析，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。本阶段主要的防护措施是数据加密，通过密码技术解决通信安全问题，从而保证数据的保密性和完整性。

2. 计算机安全（COMPUSEC）和信息安全（INFOSEC）阶段

20世纪70年代，过渡到了计算机安全阶段，其主要标志是1977年美国国家标准局（NBS）公布的《国家数据加密标准》（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）。

进入20世纪80年代后，计算机的性能得到了极大提高，应用范围不断扩大，遍及世界

各个角落，利用通信网络实现了计算机的互联和资源共享。但是，计算机信息的安全问题也随之变得越来越严重。计算机在处理、存储、传输和使用信息上存在严重的脆弱性，很容易遭受干扰、滥用或丢失，甚至被泄露、窃取、篡改、冒充或破坏。

计算机安全阶段初期的主要任务是确保计算机系统中的硬件、软件在处理、存储、传输信息过程中的保密性。其主要安全威胁来自于信息的非授权访问，主要保护措施采用安全操作系统的可信计算基（TCB）技术，本阶段仍主要考虑信息保密性的安全要求。但随着计算机病毒、计算机软件 Bug 等问题的不断出现，计算机安全中，除了保密性的安全要求外，还提出了对完整性和可用性等方面的安全要求。

国际标准化组织（ISO）将计算机安全定义为："为数据处理系统建立的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。"

进入 20 世纪 90 年代后，通信和计算机技术的进一步发展，尤其是Internet的快速发展和普及，人们对安全要求的关注对象逐步从计算机转向更具本质性的信息本身，信息安全的概念随之产生。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并限制非授权用户的服务，包括必要的检测、记录和抵御攻击的措施。除了保密性、完整性和可用性之外，人们对安全性有了可控性和不可否认性等新的要求。

国际标准化组织（ISO）将信息安全定义为："保持信息的保密性，完整性，可用性；另外也可包括诸如真实性，可核查性，不可否认性和可靠性等。"

3. 信息保障（IA）阶段

20 世纪末 21 世纪初，信息系统遭受的攻击日趋频繁，人们对信息安全概念的理解有了新的变化。

安全不再局限于信息的保护，人们需要的是对整个信息和信息系统的保护和防御，包括保护（protect）、检测（detect）、反应（react）和恢复（restore）4 个方面的能力。

安全的相对性、动态性更加引起关注，追求适度风险的信息安全成为人们的共识。安全不仅仅以功能或机制的强度作为评判指标，结合应用环境和应用需求，更加强调安全是一种信心的度量，使信息系统的使用者确信已达到预期的安全目标。

针对安全概念的新变化，1996 年美国国防部在国防部令 S－3600.1 中最早提出了"信息保障"的概念，将"信息保障"定义为："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。"这个定义强调了信息保障不仅是对信息的保障，而且包括对信息系统的保障，并明确了信息安全的 5 个属性，即可用性、完整性、保密性、鉴别性、不可否认性，提出了 4 个动态的信息安全环节，即保护、检测、反应和恢复。与早期的信息安全概念相比较，信息保障的内涵更符合现在对信息安全的要求，体现未雨绸缪、积极防御的思想。

在信息保障研究中，美国军方走在世界前列，其代表性著作之一是美国国家安全局（National Security Agency，简称 NSA）于 2000 年 9 月发布的《信息保障技术框架》3.0 版（*information assurance technical framework*），该文献于 2002 年 9 月更新为 3.1 版。此外，美国军方还于 2002 年 10 月和 2003 年初先后颁布了信息保障指导方针，即国防部第 8500.1 号令《信息保障》和第 8500.2 号令《信息保障的实施》，以指导全军的信息保障工作。

信息保障是信息安全发展的最新阶段，人们习惯上仍沿用"信息安全"的称谓。为了加

以区分，同时体现继承性，也可称为用“信息安全保障”。

信息保障除强调信息安全的保护能力外，更加重视系统的入侵检测能力、系统的事件反应能力以及系统遭受破坏后的快速恢复能力，关注的是信息系统整个生命周期的防御和恢复。

1.1.3 信息安全的概念

信息安全经历了长期的发展过程，人们对它的认识、理解比较全面透彻，下面给出目前我国研究人员比较认可的信息安全（或称信息安全保障）的概念。

信息安全保障是对信息和信息系统的安全属性、功能、效率进行保障的动态行为过程。运用源于人、技术、管理等因素所形成的保护能力、检测能力、反应能力和恢复能力，在信息和信息系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施的可用性、完整性、保密性、可控性、不可否认性等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。

上述概念中，明确了信息安全的工作范畴、安全属性、保障对象、工作环节和保障核心，有利于人们对信息安全概念的理解。

1.2 信息安全体系结构

什么是体系结构？体系结构一词由英文单词 architecture 翻译而来，在英语中最常用的解释就是“建筑”。与“建筑”相类似，一个体系结构应该包括一组构件以及构件之间的联系。在辞海中，对于体系的解释为“若干有关事物互相联系互相制约而构成的一个整体，如理论体系、语法体系、工业体系”。由此可见，体系结构强调的是：系统由若干部分构成，各部分之间存在相互关系，并组成一个整体。常见的如计算机体系结构、网络体系结构等。

前面的信息安全概念，指出信息安全是对信息和信息系统的安全属性、功能、效率进行保障的动态行为过程。不能离开信息所依赖的信息系统环境，孤立和单纯地去寻求直接保护信息内容的方式。由于信息依赖信息系统而存在，所以本书中谈及的信息安全是针对信息系统而言的，研究信息安全体系结构实际就是研究信息系统安全体系结构。换句话说，有了一个安全的信息系统，其中的信息的安全性就得到了保证，也就解决了信息安全的问题。

信息系统安全是一个多维、多层次、多因素、多目标的体系，是确保信息系统结构安全，与信息系统相关的元素安全，以及与此相关的各种安全技术、安全服务和安全管理的总和。只有信息系统安全体系结构才更具有体系性、可设计性、可实现性和可操作性。

1.2.1 信息安全体系结构模型

图 1-1 给出了信息安全体系结构的三维模型，包括安全要素、安全单元和安全过程 3

个维度，并都遵循国家和行业的相应政策、法规和标准。分析信息安全体系结构时，离不开人、技术和管理3大安全要素，设计信息安全体系结构时，需要从物理安全、系统安全、网络安全和应用安全4个安全单元来考虑，安全体系结构遵循多层次、动态的安全过程，从保护、检测、反应和恢复4个层次的纵深防御体系，通过安全策略的改进体现一个循序渐进的动态过程。

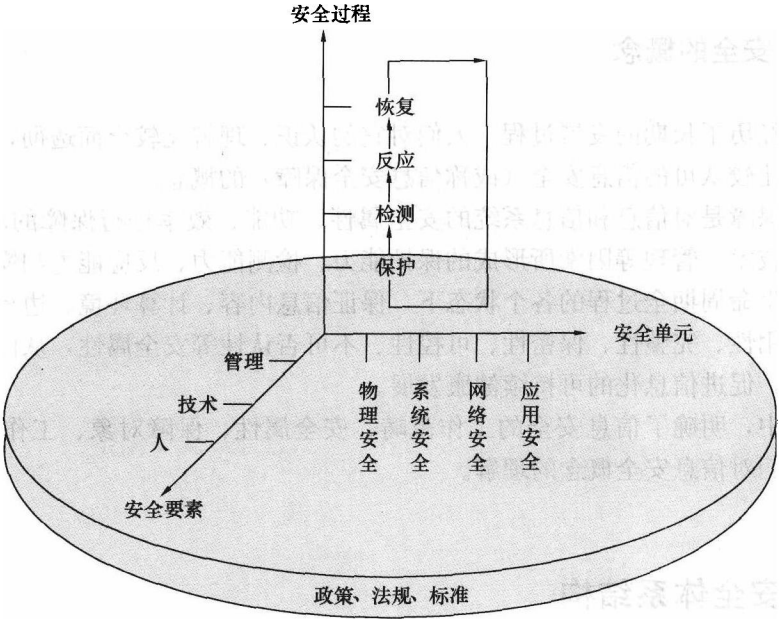

图1-1 信息安全体系结构模型

1. 安全要素

信息安全体系结构的分析设计离不开人、技术和管理3大要素，3个要素相辅相成，缺一不可。

(1) 人。信息系统的整个生命周期都离不开人的参与，包括信息系统的设计、开发、测试和维护人员，信息系统的用户，针对信息系统进行攻击和破坏的黑客，计算机病毒的制造者、传播者，信息安全事件的报告、分析、处理人员，以及信息安全法律顾问等。

影响信息系统安全的因素，除了少数难以预知的和无法抗拒的自然灾害外，绝大多数的安全威胁都与人有关，如信息系统设计人员的经验不足导致系统设计上的缺陷；开发人员的失误导致系统漏洞；有意对信息系统进行攻击和破坏的黑客；用户无意的操作失误；安全事件的报告、分析和处理人员的经验不足导致判断处理不当等，都会造成信息系统的安全问题，因此，人始终是影响信息系统安全的最大因素。全面提高信息系统相关人员的技术水平、道德品质和安全意识是信息系统安全的最重要保证。

(2) 技术。信息安全具有对抗性，技术是确保信息安全的一个重要因素。由于历史的原因，在信息技术领域，我国的自主可控能力依然很低，特别是缺乏自主可控的CPU（中央处理器）、操作系统、数据库、高端设备等，无法打破国外企业的长期垄断局面。因此，信息技术的自主可控等同于国家安全，对信息技术不能自主可控，对国家安全就不能自主可控。从国家层面来看，需要大力发展技术，提高技术产品的自主可控能力，保证国家安全和

信息安全。

对于一般的信息系统建设而言，可选择技术相对成熟、先进的产品。为了能够正确运用这些技术和合理部署相关产品，机构应建立一套有效的技术与产品采购策略和过程，具体包括制定安全策略、信息安全保障原则、信息保障产品选用准则、经可信第三方认证的产品采购原则、产品配置，以及进行系统风险评估等。

(3) 管理。管理是确保信息安全的另一个重要因素，从理论上看，不存在绝对安全的技术，技术固然重要，但管理更不容忽视。虽然“三分技术，七分管理”的说法不一定准确，但却能够说明管理的重要性。从目前我国实际发生的安全事件看，较为薄弱的还是信息安全管理，很多信息安全事件都是由于管理不到位、责任不落实造成的。因此，建立信息安全管理机构，加强组织协调，发挥其统筹规划、科学管理、宏观调控和决策的作用，强化信息安全管理，形成全方位的信息安全管理体系至关重要。有关信息安全管理的内容将在第7章详细介绍。

坚持管理和技术并重，做到管理手段和技术手段相结合，也就是在加强管理的前提下，采用先进的安全技术，在提升技术的基础上强化管理。

2. 安全单元

信息安全体系结构主要有4个层面的安全单元。

(1) 物理安全。物理安全又叫实体安全（physical security），是保护计算机设备、设施（网络及通信线路）免遭地震、水灾、火灾、有害气体或其他环境事故（如电磁污染等）破坏的措施和过程。

(2) 系统安全。系统安全就是对计算机系统的硬件、软件和数据加以保护，不因偶然的或者恶意的原因而造成破坏、更改或泄露，使计算机系统得以连续正常地运行。

(3) 网络安全。网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不被偶然的或者恶意的原因破坏、更改或泄露，系统连续可靠正常地运行，网络服务不中断。广义来说，凡是涉及网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是网络安全所要研究的领域。

(4) 应用安全。应用系统的安全是安全建设最主要的目的。信息总是通过应用系统来存取的，所以应用系统的安全是确保信息安全的根本。

3. 安全过程

安全过程遵循PDRR安全模型，包括保护（protect）、检测（detect）、反应（react）和恢复（restore）4个部分，他们构成了一个动态的信息安全周期，其中每一部分都有相应的安全策略来支持，如图1-2所示。

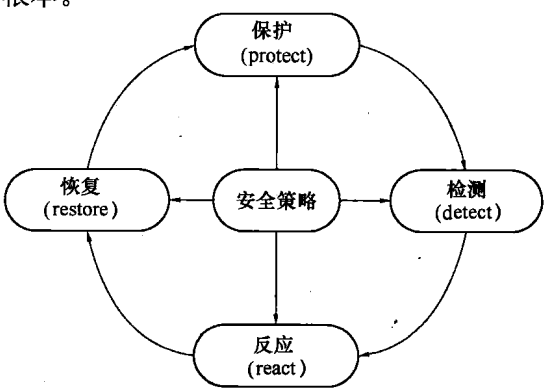

图1-2 PDRR安全模型

(1) 保护。保护是PDRR模型的最重要部分，他预先阻止攻击可以发生的条件，让攻击者无法顺利地入侵，保护可以减少大多

数的入侵事件。

(2) 检测。检测是 PDRR 模型中的第二个环节。前面环节的保护系统可以除掉入侵事件发生的条件，一般能阻止绝大多数入侵事件的发生，但是他不能阻止所有的入侵，尤其是一些针对新的系统缺陷、新的攻击手段的入侵。因此，一旦入侵发生，就通过检测环节检测出来，常用的检测工具就是 IDS（入侵检测系统）。

(3) 反应。反应是 PDRR 模型中的第三个环节，是在已知一个攻击（入侵）事件发生之后所进行的处理。在一个大规模的网络中，反应工作都由一个特殊部门负责，即计算机应急响应小组（CERT）。

(4) 恢复。恢复是 PDRR 模型中的最后一个环节，是当攻击（入侵）事件发生后，把系统恢复到原来的状态，或者比原来更安全的状态。恢复可以分为系统恢复和信息恢复两种方式。系统恢复指的是修补该攻击（入侵）事件所利用的系统缺陷，包括系统升级、软件升级和打补丁等，避免黑客再次利用这样的缺陷入侵；信息恢复就是从备份和归档的数据中恢复出原来数据。

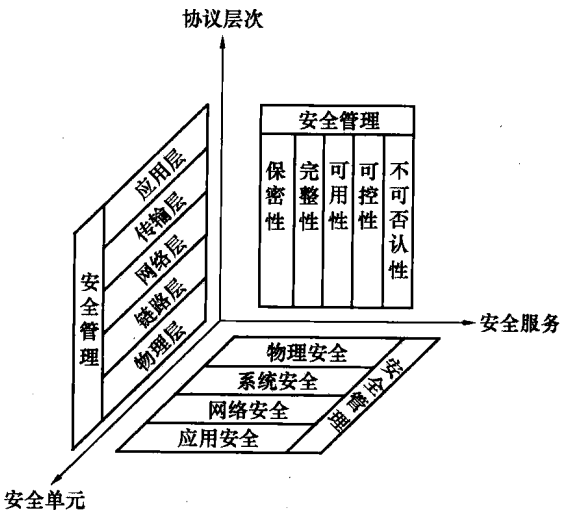

图 1-3 信息安全技术体系结构

1.2.2 信息安全技术体系

图 1-3 给出了信息安全技术体系结构，借鉴了美国国防部信息系统安全计划（DISSP）提出的三维安全体系结构的思路，将安全服务、安全单元和协议层次作为三维坐标系中的 3 个维度。安全服务包括保密性、完整性、可用性、可控性和不可否认性；安全单元包括物理安全、系统安全、网络安全和应用安全；协议层次包括可配置安全服务的 5 个层次，即物理层、链路层、网络层、传输层和应用层。另外，每一维度都有相应安全管理的要求。每一种安全服务可对应到相应的协议层次，也可对应到相应的安全单元，不同的安全单元对应到相应的协议层次。

1.3 我国的信息安全对策

1.3.1 信息安全对策

随着我国国民经济和社会信息化进程的全面加快，网络与信息系统的基础性、全局性作用日益增强，信息安全已经成为国家安全的重要组成部分。党和政府对信息安全高度重视，

并提出了具体要求，标志着我国信息安全保障工作有了基本纲领和大政方针，明确了指导思想和主要任务。

1. 总体要求

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，立足于安全防护，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，积极防御还要求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。

2. 主要原则

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，强化基础性工作；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。

3. 主要任务

我国信息安全保障工作的主要任务是：

① 实行信息安全等级保护；

② 加强以密码技术为基础的信息保护和网络信任体系建设；

③ 建设和完善信息安全监控体系；

④ 重视信息安全应急处理工作；

⑤ 加强信息安全技术研究开发，推进信息安全产业发展；

⑥ 加强信息安全法制建设和标准化建设；

⑦ 加快信息安全人才培养，增强全民信息安全意识；

⑧ 保证信息安全资金；

⑨ 加强对信息安全保障工作的领导，建立健全信息安全管理责任制。

1.3.2 信息化发展战略

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），分析了全球信息化发展的基本趋势和我国信息化发展的基本形势，提出了我国信息化发展的指导思想、战略目标、战略重点、战略行动计划和保障措施。把建设国家信息安全保障体系作为我国信息化发展的战略重点，为我国的信息安全保障工作指明了方向。

在11号文件中“建设国家信息安全保障体系”部分，有如下2方面的要求。