高等院校应用型人才培养规划教材

网络与信息安全实用教程

唐 华 主编　　夏 旭 副主编

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

高等院校应用型人才培养规划教材

网络与信息安全实用教程

唐　华　主　编
夏　旭　副主编

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书全面地介绍了计算机网络安全与信息安全技术。全书共 10 章，内容包括：网络安全概述、操作系统安全配置、密码学技术基础、VPN 技术、防火墙技术、恶意代码分析与防范、网络攻击与防范、入侵检测技术、应用服务安全和数据库安全等内容。每章都配有习题、详细的实训项目及思考题，从而有针对性地帮助读者理解本书的内容。

本书可作为本科院校、高等职业院校计算机及其相关专业“网络安全技术”类课程教材，也可供相关的技术人员参考。

图书在版编目（CIP）数据

网络与信息安全实用教程/唐华主编. —北京：电子工业出版社，2014.1
高等院校应用型人才培养规划教材
ISBN 978-7-121-21955-9

Ⅰ. ①网… Ⅱ. ①唐… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字（2013）第 276800 号

策划编辑：吕 迈
责任编辑：王凌燕
印 刷：三河市鑫金马印装有限公司
装 订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1 092 1/16 印张：22 字数：563.2 千字
印 次：2014 年 1 月第 1 次印刷
印 数：3 000 册 定价：39.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着互联网的飞速发展，尤其是这几年来移动互联网、社交网络及大数据应用的逐渐普及，计算机网络已经渗透到人们日常生活的方方面面，人们的工作与生活已经离不开网络了。在享受网络带来的便利的同时，网络的安全问题也日渐突出。例如，非法侵入计算机系统窃取机密信息、篡改和破坏数据、病毒、蠕虫、垃圾邮件、僵尸网络等。网络安全已关系到国家安全和社会稳定等重大问题。

本书是面向网络的安全教材，充分考虑了高职高专院校学生的特点。在编写本书时，作者注重贯穿能力和技能培养，针对网络信息安全的理论知识和工作原理介绍得较少一些，侧重理论联系实际与工程实践技能的培养，加大了网络安全技术的应用和相关操作技能方面的知识。

本书作者经过多年教学、产学研的实践，并融合了作者多年本门课程教学改革的成果，在编写中，通过引例引出该章实际待解决的问题，每章的内容力求反映最新的网络安全技术的现状及发展趋势。在每章后还增加了详细的实训内容，包括实训目的、实训要求、实训环境和详细的实训步骤等内容，使学生通过实训项目进一步引导对理论的学习。

为了加深对知识的理解和便于教学，在每章课后还安排了各种类型的习题以及实训思考题，使学生不仅能及时了解自己对相关理论知识的掌握程度，也能进一步熟悉和掌握相关网络安全技术的应用，及时消化吸收所学的知识。

本书由华南师范大学软件学院的唐华任主编，湖南安全技术职业学院的夏旭任副主编，其中唐华编写第 4 章和第 6 章至第 9 章，并对全书进行了统稿和审校；夏旭编写了第 1 章、第 2 章和第 10 章，并参与了其他部分章节的修改。湖南安全技术职业学院的罗危立和王磊老师分别编写了第 3 章和第 5 章。本书编委会成员有：杜瑛、许烁娜、胡绪英、易明珠、邓虹、杨桂芝、舒纲旭、梁艳、陈俊、吴干华、张倩华、冼广铭、杨洋、吴锐珍、杨滨、皱竞辉、邓惠、王路露、刘青玲、丁美荣。

为便于教学，本书提供 PPT 课件、习题解答及本书所涉及的相关软件。这些资源可在电子工业出版社的网站下载，也可联系作者。作者的电子邮箱是 karma2001@163.com，欢迎大家交流。

由于作者水平有限，加之网络安全技术发展变化快，书中不足之处在所难免，恳请读者提出宝贵意见，以帮助我们将此教材进一步完善。

编　者

2013 年 8 月

反侵权盗版声明

举报电话：（010）88254396；（010）88258888
传　　真：（010）88254397
E-mail：　dbqq@phei.com.cn
通信地址：北京市万寿路 173 信箱
　　电子工业出版社总编办公室
邮　　编：100036

目 录

CONTENTS

第1章 网络安全概述

【知识要点】

通过对本章的学习，理解信息安全和网络安全的基本概念，初步了解网络安全的防护体系、评价标准及法律法规。本章主要内容如下：

- 信息安全定义
- 网络安全定义
- 网络安全防护体系

【引例】

生活在今天的人们，常常能听到关于黑客的故事，而且都具有传奇的色彩：一位少年黑客通过互联网闯入美国五角大楼，窃取原子弹核心技术资料，引起恐慌；一名黑客将美国司法部主页上的“美国司法部”改成了“美国不公正部”。

最近发生的具有代表性的黑客事件是2013年2月6日，美联储发布声明称其内部网站被入侵。一个名为匿名者（Anonymous）的黑客组织在周日侵入了美联储网站，得到了4000余位银行高管的个人信息并将其公布在网上。匿名者黑客组织的典型形象如图1.1所示。

图1.1 匿名者（Anonymous）黑客组织

2013年4月24日，美联社的官方推特（Twitter）账号遭黑客入侵并发布白宫发生两起爆炸、奥巴马总统受伤的假新闻，这条假消息令美股盘中大幅波动，美股在稳定上涨的情况下猛然下挫，道指2分钟重挫140余点。

事实上，这些网络入侵事件只是实际所发生的事件中非常微小的一部分，相当多的网络入侵并没有被人们发现，可以说，在现在的互联网上，没有任何事情可以绝对相信，即使是收到的一封邮件，也有可能不是真实的。

今天，网络和主机是否容易遭受攻击，已经成为网络世界最关注和时髦的话题。网络安全不仅仅是研究者讨论的课题，也是全球互联网建设者和使用者所关心的话题。

1.1 信息安全概述

在席卷全球的信息化浪潮中，信息技术作为推动社会发展的强有力因素，已经成为世界经济增长的重要动力。随着信息网络覆盖面的扩大，信息安全问题所造成的影响与后果也随之增大。目前，信息的获取、处理和安全的保障能力已经成为一个国家综合国力的重要组成部分。信息安全事关国家安全和社会稳定，因此，必须采取措施确保我国的信息安全。

1.1.1 信息安全概述

随着信息化的发展，有关“信息安全”的定义，日益引起争议。在 2001 年 11 月的第 56 届联大会议中，曾呼吁所有会员国就“有关信息安全的各种基本概念的定义”向秘书长进行通报，其目的就是旨在消除概念上的混乱，更好地促进信息安全的国际性合作，然而，到目前为止，国际上仍没有一个权威、公认的有关“信息安全”的标准定义。

国际上信息安全的英文有 Information Security 和 Cyber Security 两种表述方式，在不同的信息化发展阶段及从不同的认识角度出发，有多种对信息安全的定义，以下列举三种常见的定义。

定义 1：维基百科中，信息安全是指为保护信息及信息系统免受未经授权的进入、使用、披露、破坏、修改、检视、记录及销毁。

定义 2：美国国家安全电信和信息系统安全委员会（NSTISSC）定义信息安全是对信息、系统及使用、存储和传输信息的硬件的保护，是所采取的相关政策、认识、培训和教育及技术等必要手段。

定义 3：这种定义将信息安全所涉及的内容具体化，认为信息安全是确保存储或传送中的数据不被他人有意或无意地窃取和破坏，这种定义将信息安全分解为 4 个方面，分别是信息设施及环境安全、数据安全、程序安全及系统安全。

总的来说，信息安全的概念是在不断变化、发展和完善的。其内涵所涉从最初的军事领域和军队等特定群体迅速扩展到信息化时代社会生活的各个方面。

需要注意的是，信息安全这一术语，与计算机安全和信息保障（Information Assurance）等术语经常被不正确地互相替换使用。事实上，这些领域的确相互关联，并且拥有一些共同的目标——保护信息的机密性、完整性和可用性，但是，它们之间仍然有一些微妙的区别。

其区别主要在于达到这些目标所使用的方法及策略，以及所关心的领域。信息安全主要涉及数据的机密性、完整性、可用性，而不管数据的存在形式是电子的、印刷的还是其他的形式。

信息安全的领域在最近这些年经历了巨大的成长和进化。它提供了许多专门的研究领域，包括安全的网络和公共基础设施、安全的应用软件和数据库、安全测试、信息系统评估、企业安全规划及数字取证技术等。

1.1.2 信息安全的基本要求

虽然，目前仍然没有信息安全的标准定义，但是，由于信息安全的最根本属性是防御性的，因此，信息安全的基本要求主要是数据的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability），即 CIA，如图 1.2 所示。其含义如表 1.1 所示。

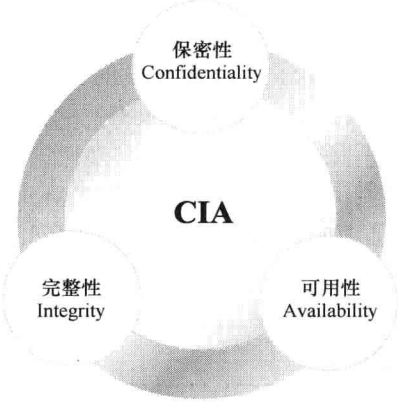

图 1.2 信息安全的基本要求

表 1.1 信息安全基本要求的含义

基本要求	含义	举例
保密性	确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体	事件 1：你不希望别人知道在银行有多少存款 事件 2：你不希望竞争对手知道你这次项目的报价
完整性	确保信息在存储、使用、传输过程中不会被非授权用户篡改，防止授权用户或实体不恰当地修改信息，保持信息内部和外部的一致性	事件 1：你不希望突然有一天发现钱变少了 事件 2：你不希望你的项目报价数目突然被篡改了
可用性	确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源	事件 1：你肯定希望自己能随时使用这笔钱 事件 2：你肯定希望自己能随时获取项目的所有资料

以上三要素又被称为信息安全的“金三角”。为了保障信息的保密性，常用的技术包括：信息加密、物理保密和信息隐形等；为了保障信息的完整性，常用的技术包括：数字签名、数字印章和密码校验等；为了保障信息的可用性，常用的技术包括：双机热备、数据备份和恢复等。

除了 CIA，信息安全的基本要求还包括信息的可控性和可审查性。可控性指可以对授

权范围内的信息进行审计、跟踪、检测和控制；可审查性指采用审计、监控等安全机制，使得信息使用者的行为有证可查，并可以对出现的网络安全问题提供调查的依据和手段。

1.1.3 信息安全的发展

信息安全的概念和技术是随着人们的需求，随着计算机、通信与网络等信息技术的发展而不断变化的。大体可以分为数据安全、网络信息安全和交易安全三个阶段，如图 1.3 所示。

1．数据安全阶段

这一阶段是计算机的基本安全要求，依赖的基本技术是密码。

早在几千年前，人类就会使用加密的办法传递信息。1988 年，美国康奈尔大学学生罗伯特·莫里斯研制了世界上第一个蠕虫，如图 1.4 所示。在“蠕虫”事件发生以前，信息保密技术的研究成果主要包括两类，一类是发展各种密码算法及其应用；另一类是计算机信息系统保密性模型和安全评价准则。主要开发的密码算法有：1977 年美国国家标准局采纳的分组加密算法 DES（数据加密标准）；双密钥的公开密钥体制 RSA，该体制是根据 1976 年 Diffie 和 Hellman 在“密码学新方向”开创性论文中提出来的思想，由 Rivest、Shamir 和 Adleman 三人创造的；1985 年 N.koblitz 和 V.Miller 提出了椭圆曲线离散对数密码体制（ECC），该体制的优点是可以利用更小规模的软件、硬件实现有限域上同类体制的相同安全性；另外，还创造出一批用于实现数据完整性和数字签名的杂凑函数，如数字指纹、消息摘要（MD）、安全杂凑算法（SHA——用于数字签名的标准算法）等，其中有的算法是 20 世纪 90 年代提出的。

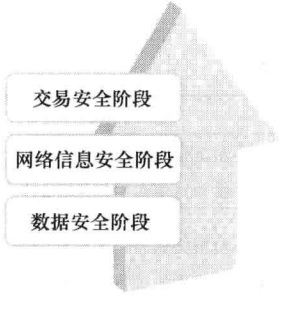

图 1.3 信息安全的发展

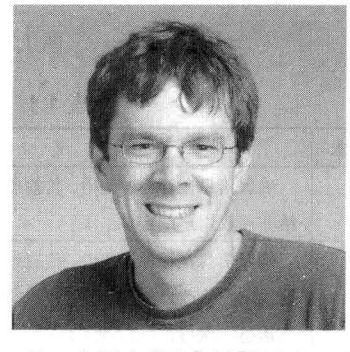

图 1.4 第一个蠕虫病毒制造者 Robert Morris

2．网络信息安全阶段

这是网络时代最基本安全要求，依赖的基本技术是防护技术。

由于互联网的开放性及快速普及，使得信息暴露在更多用户面前。信息安全问题日益严重，此时，不仅需要考虑信息系统本身的安全问题，还需要考虑可能来自网络环境的攻击造成的问题。1988 年 11 月 3 日，莫里斯“蠕虫”造成 Internet 几千台计算机瘫痪的严重网络攻击事件，引起了人们对网络信息安全的关注与研究，并在 1989 年成立了计算机紧急事件处理小组负责解决 Internet 的安全问题，从而开创了网络信息安全的新阶段。在

该阶段中，除了采用和研究各种加密技术外，还开发了许多针对网络环境的信息安全与防护技术，这些防护技术是以被动防御为特征的。其主要包括以下几种技术。

（1）安全漏洞扫描器：用于检测网络信息系统存在的各种漏洞，并提供相应解决方案。

（2）安全路由器：在普通路由器的基础上增加更强的安全性过滤规则，增加认证与防瘫痪性攻击的各种措施。安全路由器完成在网络层与传输层的报文过滤功能。

（3）防火墙：在内部网与外部网的入口处安装堡垒主机，在应用层利用代理功能实现对信息流的过滤功能。

（4）入侵检测系统（IDS）：根据已知的各种入侵行为的模式判断网络是否遭到入侵的系统，一般也同时具备告警、审计与简单的防御功能。

（5）各种防网络攻击技术：其中包括网络防病毒、防木马、防口令破解、防非授权访问等技术。

（6）网络监控与审计系统：监控内部网络中的各种访问信息流，并对指定条件的事件做审计记录。

当然在这个阶段中还开发了许多网络加密、认证、数字签名的算法和信息系统安全评价准则（如 CC 通用评价准则）。这一阶段的主要特征是对于自己部门的网络采用各种被动的防御措施与技术，目的是防止自身内部网络受到攻击，保护内部网络的信息安全。

3. 交易安全阶段

这是网络电子交易时代最基本的安全要求，以可信性为主，实施的是自愿型保障策略。

交易安全阶段也可以称为信息保障阶段，信息保障（IA）这一概念最初是由美国国防部长办公室提出来的，后被写入命令《DoD Directive S-3600.1:Information Operation》中，在 1996 年 12 月 9 日以国防部的名义发表。在这个命令中信息保障被定义为：通过确保信息和信息系统的可用性、完整性、可验证性、保密性和不可抵赖性来保护信息系统的信息作战行动，包括综合利用保护、探测和反应能力以恢复系统的功能。1998 年 1 月 30 日，美国国防部批准发布了《国防部信息保障纲要》（DIAP），纲要中认为信息保障工作是持续不间断的，它贯穿于平时、危机、冲突及战争期间的全时域。信息保障不仅能支持战争时期的国防信息攻防，而且能够满足和平时期国家信息的安全需求，如电子商务的安全交易。

信息保障（IA）依赖于人、技术及运作三者去完成任务，还需要掌握技术与信息基础设施。要获得健壮的信息保障状态，需要通过组织机构的信息基础设施的所有层次的协议去实现政策、程序与技术。

1.2　网络安全概述

由于互联网所具有的开放性、国际性和自由性，在实现信息资源最大程度共享的同时，安全问题也日渐凸显。如何保护内部机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所必须考虑的重要问题。

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，不受偶然的或恶意

的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

需要注意的是网络安全和信息安全的区别，信息安全涵盖的范围更广，包括了网络安全、系统安全、数据安全及物理安全等所有和信息相关的安全问题，而网络安全则仅是信息安全中与网络相关的一部分安全问题，两者区别如表 1.2 所示。

表 1.2 信息安全与网络安全的区别

名 称	涵 盖 范 围	区 别
信息安全	网络安全、系统安全、数据安全、物理安全及和安全管理相关的策略管理、业务管理、人员管理、安全法律法规等	信息安全更为宏观，包括了网络安全。信息安全是包括人员、技术和管理三要素的系统工程，而网络安全更偏重网络层面的安全
网络安全	网络设备安全、连接线路安全等	

1.2.1 网络安全模型

网络安全模型是动态网络安全过程的抽象描述。为了达到安全防范的目标，需要建立合理的网络安全模型。目前，网络安全领域存在较多的安全模型，各模型各有侧重，被应用到不同的领域，本节将介绍网络安全领域的基本模型、P2DR 模型和 PDRR 模型。通过学习网络安全模型，构建合理的网络安全防护体系。

1. 基本模型

在网络信息传输中，为了保证信息传输的安全性，需要构建一个值得信任的第三方，负责向源节点和目的节点进行秘密信息的分发，同时当发送方和接收方发生争执时，可以进行仲裁。图 1.5 为网络安全基本模型的示意图。可以通过以下实例对该模型进行说明：

用户 A 将产品卖给不认识的用户 B，B 希望通过支票付款，但是用户 A 不知道支票的真假，同样，用户 B 也不相信用户 A，在没有获得产品所有权时，不愿意将支票交给用户 A，此时，两位用户可以通过双方都信任的第三方机构或个人进行交易，用户 A 将产品交给第三方，用户 B 将支票交给用户 A，用户 A 在银行兑现支票，在支票兑现无误后，由第三方将产品交给用户 B，如果支票在规定时间内无法兑换，用户 A 将出示证据给第三方，第三方将产品退还给用户 A。

2. P2DR 模型

P2DR 模型是最先发展起来的一个动态安全模型，该模型由美国国际互联网安全系统公司 ISS 提出，即 Policy（策略）、Protection（防护）、Detection（检测）和 Response（响应）。根据 P2DR 模型的观点，一个完整的动态安全体系，不仅需要恰当的防护（例如，操作系统访问控制、防火墙、加密技术等），而且需要动态的检测机制（例如，入侵检测、漏洞扫描等），在发现问题时还需要及时响应，这样的体系需要在统一的、一致的安全策略指导下实施，形成一个完备的、闭环的动态自适应安全体系。该模型可以用图 1.6 表示。

在 P2DR 模型中，恢复（Recovery）环节是包含在响应（Response）环节中的，作为事件响应之后的一项处理措施，不过，随着人们对业务连续性和灾难恢复愈加重视，尤其是“9 • 11”恐怖事件发生之后，人们对 P2DR 模型的认识也就有了新的内容，于是，

PDRR 模型就应运而生了。

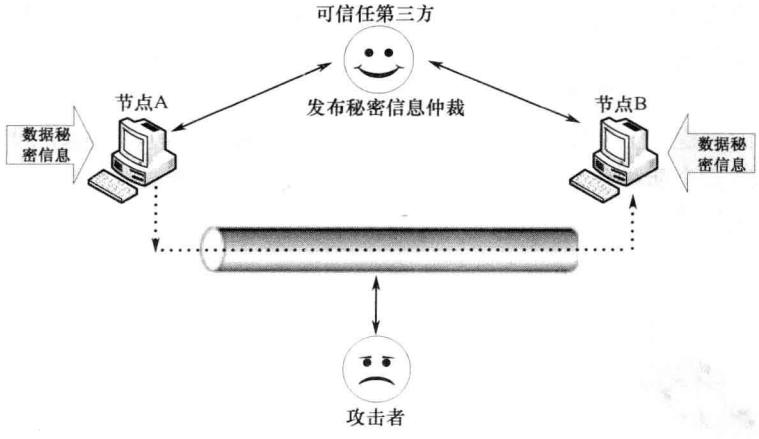

图 1.5　网络安全基本模型

3．PDRR 模型

PDRR 模型与 P2DR 模型唯一的区别就是将恢复环节单独列出。在 PDRR 模型中，安全策略、防护、检测、响应和恢复共同构成了完整的安全体系，如图 1.7 所示。

图 1.6　P2DR 模型

图 1.7　PDRR 模型

防护、检测、响应和恢复这 4 个阶段并不是孤立的，构建信息安全保障体系必须从安全的各个方面进行综合考虑，只有将技术、管理、策略、工程过程等方面紧密结合，安全保障体系才能真正成为指导安全方案设计和建设的有力依据。

PDRR 也是基于时间的动态模型，其中，恢复环节对于信息系统和业务活动的生存起着至关重要的作用，各企业及机构只有建立并采用完善的恢复计划和机制，其信息系统才能在重大灾难事件中尽快恢复并延续业务。

1.2.2　网络安全的防护体系

根据艾瑞咨询 2012 年对网民调研的结果显示，越来越多的网民已经意识到网络安全的重要性，70%的网民对网络安全表示担心，其中 33.3%持非常担心态度，调研结果如图 1.8 所示。因此，需要构建完善的网络安全防护体系。

通过对网络安全模型的了解，可以发现网络安全是一项系统工程，它不是一些网络安全产品的简单堆叠，网络安全包括了硬件、软件、网络、人及之间相互关系和接口等多个组成部分。本节提出一种动态、多层次的网络安全防护体系，该体系包括安全政策、安全技术、安全管理和法律法规 4 个部分，如图 1.9 所示。在该体系中，安全政策是中心，安全管理是落实的关键，安全技术是实现网络安全防范的技术手段和支撑，国家法律法规是后盾，可见网络安全防护体系不仅包括安全产品和技术，更重要的是需要建立包括政策、管理在内的安全体系。

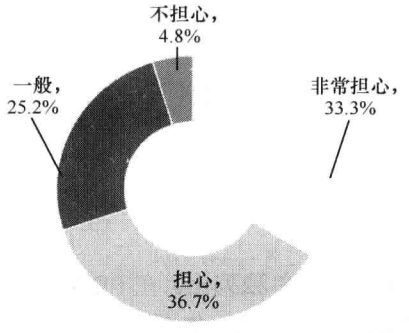

图 1.8　2012 年网民对网络安全的担忧情况

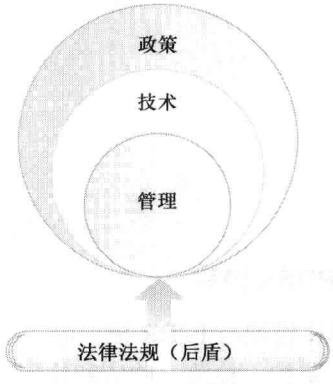

图 1.9　网络安全防护体系示意图

具体而言，该模型是以评估为基础，在评估的基础上进行安全政策的设计，然后，可以确定需要采用的安全技术和工具，从而构成以评估、防护、检测、响应和恢复为技术支撑和实现手段的网络安全防护体系，为了保障防护体系的持续性稳定运行，需要使用合理的管理手段，确保体系能发挥应有的作用。整个防护体系的逻辑关系图如图 1.10 所示。

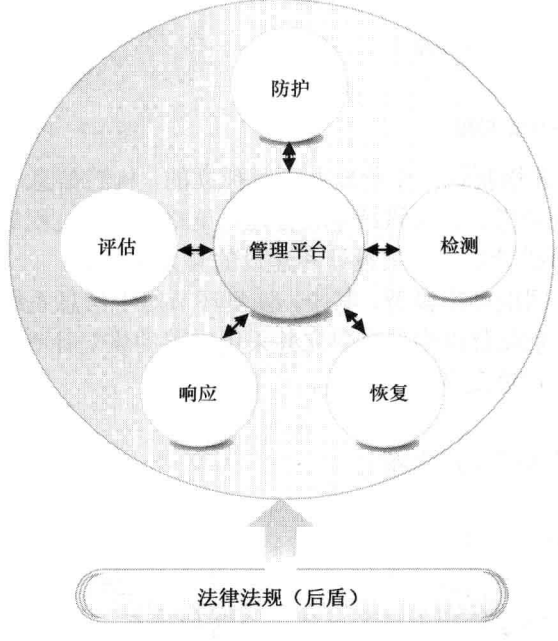

图 1.10　网络安全防护体系逻辑关系图