高等院校信息安全专业规划教材

网络信息安全

- 信息安全的三个基本控制理论——访问控制原理、信息流控制原理和推理控制原理
- 计算机硬件、操作系统、计算机网络、数据库系统和应用系统各个层次上的信息安全机制和技术
- 成熟的信息安全理论与最新的研究成果

提供电子教案

肖军模　刘　军　周海刚　等编著

机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

网络信息安全

肖军模　刘　军　周海刚　等编著

机械工业出版社

本书重点论述了访问控制、信息流控制和数据库推理泄漏控制等信息安全的基本理论与方法，讨论了信息系统的安全模型和等级评价标准，系统地分析了计算机硬件、操作系统、网络及其安全设备、数据库系统和应用系统的安全机制的原理及其可能存在的安全缺陷。书中还比较详细地介绍了安全操作系统和安全应用系统的设计与开发方法，同时简要介绍了各种常用的加密技术。

本书可以作为信息安全专业、计算机专业、信息工程专业及相关专业的本科生或研究生教材，也可以作为从事网络信息安全领域的科技人员与信息系统安全管理员的参考书。

图书在版编目（CIP）数据

网络信息安全/肖军模等编著. —北京：机械工业出版社，2006.1
高等院校信息安全专业规划教材
ISBN 7-111-17749-5

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

中国版本图书馆 CIP 数据核字（2005）第 126103 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：胡毓坚 责任编辑：赵 慧 版式设计：张世琴
责任校对：樊钟英 封面设计：刘吉维 责任印制：洪汉军
北京瑞德印刷有限公司印刷
2006 年 1 月第 1 版第 1 次印刷
787mm×1092mm 1/16 · 23 印张 · 568 千字
0 001—5 000 册
定价：32.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68326294
封面无防伪标均为盗版

高等院校信息安全专业规划教材

编委会成员名单

出版说明

信息技术的发展和推广，为人类开辟了一个新的生活空间，它正对世界范围内的经济、政治、科教及社会发展各方面产生重大的影响。如何建设安全的网络空间，已成为一个迫切需要人们研究、解决的问题。目前，与此相关的新技术、新方法不断涌现，社会也更加需要这类专门人才。为了适应对信息安全人才的需求，我国许多高等院校已相继开设了信息安全专业。为了配合相关的教材建设，机械工业出版社邀请了解放军信息工程大学、解放军理工大学通信工程学院、上海交通大学、西安电子科技大学、湖南大学、中山大学、南京邮电学院等高校的专家和学者，成立了教材编委会，共同策划了这套面向高校信息安全专业的教材。

本套教材的特色：

1. 作者队伍强。本套教材的作者都是全国各院校从事一线教学的知名教师和学术带头人，具有很高的知名度和权威性，保证了本套教材的水平和质量。

2. 系列性强。整套教材根据信息安全专业的课程设置规划，内容尽量涉及该领域的方方面面。

3. 系统性强。能够满足专业教学需要，内容涵盖该课程的知识体系。

4. 注重理论性和实践性。按照教材的编写模式编写，在注重理论教学的同时注意理论与实践的结合，使学生能在更大范围内、更高层面上掌握技术，学以致用。

5. 内容新。能反映出信息安全领域的最新技术和发展方向。

本套教材可作为信息安全、计算机等专业的教学用书，同时也可以供从事信息安全工作的科技人员以及相关专业的研究生参考。

机械工业出版社

前　言

1988 年 11 月 3 日这一天被称为“黑色的星期四”，一个美国年轻人 Robert Morris 把一个“蠕虫”程序放到了 Internet 上，导致了上千台网上机器瘫痪。这个称为“Morris 蠕虫”程序的出现改变了许多人对 Internet 安全性的看法，引起人们对计算机网络安全问题的重视。而在该事件之前，人们的信息安全概念主要是数据加密，重点是保护存储在各种介质上和传输过程中的数据。进入 20 世纪 90 年代后，Internet 走向商业化，上网计算机以翻番的速度增加，网络“黑客”与“入侵者”的非法活动呈猖獗趋势。人们发现信息安全问题无法仅用数据加密技术完全加以解决，还需要解决硬件系统、操作系统、网络、数据库系统和应用系统的整体安全问题。信息安全问题也就进入了网络信息安全阶段。网络信息安全阶段的主要特征是被动防御，采取各种措施（如防火墙、入侵检测等）来防范各种可能的入侵。进入 21 世纪后，各国对信息安全的重要性与作用有了更高的认识，美国首先提出了信息保障的概念，提出了防护、检测、反应与恢复（PDRR）模型，使信息安全进入主动防御阶段。

信息战先后在两次海湾战争中发挥了重要作用，在各国军队中产生了震动。以美国为首的外国军队加强了对信息战的研究，并已取得显著进展。我们认为信息战的主战场是计算机网络空间，谁能在计算机网络空间取得了信息的控制权，谁就在信息战中取得了主动权。为了国家的安全，我们也应该加强这一领域中各种技术的研究工作。

本书通过介绍信息安全的 3 个基本控制理论——访问控制原理、信息流控制原理和推理控制原理，分析计算机硬件与环境、操作系统、计算机网络、数据库系统和应用系统的安全机制和存在的安全缺陷，提高读者对网络安全问题的全面和系统的认识，以及在网络中的安全防范意识和防护能力，同时也为学习网络信息对抗奠定了基础。

本书可作为信息安全专业或相关专业的教材。在选材上，根据内容的系统性、完整性和实用性的需要，尽量选择成熟的和长期起作用的信息安全理论与最新的研究成果，尽量避免选择那些时效性很强的具体技术与方法（如针对某个具体系统漏洞的安全解决办法）。根据这些想法，我们广泛综合了国内外有关信息安全方面的理论与素材，以及自己的实际工作经验，按照计算机硬件、操作系统、计算机网络、数据库系统和应用系统的层次，论述各个层次上的信息安全机制和技术。

本书是在总结3届教学实践的基础上编写而成的。第1章主要论述信息安全与信息对抗的基本概念和相应技术的发展，所介绍的信息保障技术框架和纵深防御策略在今后很长时间内仍将是适用的；第2章介绍各种常用的密码技术，补充了诸如IDEA、AES、背包密码体制和椭圆曲线密码体制等内容，以反映密码技术的新发展；第3章介绍了访问控制原理及其安全模型；第4章介绍了信息流控制原理及其安全模型，并讲解了编译器中如何划分基本块的方法；第5章论述了信息系统的安全性评价标准，第6章讨论了计算机硬件、运行环境、操作系统和应用程序系统等计算机系统安全问题；第7章详细讨论了数据库推理泄漏控制原理；第8章讨论了与计算机网络有关的一些特殊安全问题。为了便于开展教学，本书配套了电子教案，下载网址为：http://www.cmpbook.com。

本书第1、3、4、5、6章由肖军模编写，第2、8两章由周海刚编写，第7章由刘军编写。肖军模负责全书的组织、主审和修改任务。需要特别说明的是，书稿的部分内容引用了南京解放军理工大学通信工程学院方世昌教授的内部教材资料。参加编写的还有王衍波、张增军、袁震、戴江山、于震伟、郭继斌、刘晶等。此外还得到了该院信息安全研究中心教员和硕士、博士研究生的支持和帮助，在此向所有为本书做出贡献的同志致以衷心的感谢。对于书中的错误和不足之处，欢迎广大读者和专家提出批评意见。作者联系方式为：025-80828450，jmxiao753@sina.com。

作　者

目　录

第1章　信息安全概述

人类已经进入信息化社会，随着 Internet 在全世界日益普及，政府、军队、企业等部门越来越需要利用网络传输与管理信息。虽然计算机与网络技术为信息的获取、传输与处理利用提供了越来越先进的手段，但也为好奇者与入侵者提供了方便之门，使得计算机与网络中的信息变得越来越不安全了。由于网络“黑客”与“入侵者”的活动越来越频繁，人们对计算机与网络中信息的安全也越来越担心了。不仅金融、商业、政府部门担心，军事部门更为担心。信息技术发展到今天，迫切要求发展各种信息安全技术。怎样才能使计算机与网络中的信息更安全，必须研究网络与计算机本身的安全机制和措施，研究“黑客”与“入侵者”的攻击方法和对他们的防范措施，这也是编写本书的主要宗旨。

1.1　信息安全与信息对抗

“信息”是一个广泛的概念，不仅包括计算机文件系统或数据库系统中存储的各种数据、正文、图形、图像、声音等形式的多媒体数据文件、软件或各种文档资料，也包括存放或管理这些信息的硬件信息，如计算机硬件及其网络地址、网络结构、网络服务等都属于本书中所涉及的“信息”。尽管在许多文献中都大量引用“数据”与“信息”两个术语，但却没有一个被公认的对数据与信息的定义。本书将不对信息与数据加以区分，信息安全与数据安全是指同一个概念。在字典中，“安全”一词是指“远离危险、威胁的状态或特性”和“为防范间谍活动或蓄意破坏、犯罪、攻击等而采取的措施。”信息安全则是指防止任何对数据进行未授权访问的措施，或者防止造成信息有意无意泄露、破坏、丢失等问题的发生，让数据处于远离危险、免于威胁的状态或特性。

1.1.1　信息的安全需求

计算机网络信息系统的安全需求主要用 4 方面表征：保密性、完整性、可用性和不可否认性。

保密性表示对信息资源开放范围的控制，不让不应涉密的人涉及秘密信息。实现保密性的方法一般是通过信息的加密、对信息划分密级，并为访问者分配访问权限，系统根据用户的身份权限控制对不同密级信息的访问。除了考虑数据加密、访问控制外，还要考虑计算机电磁泄露可能造成的信息泄露。

完整性是指保证计算机系统中的信息处于“保持完整或一种未受损的状态”。任何对系统信息应有特性或状态的中断、窃取、篡改、或伪造都是破坏系统信息完整性的行为。其中中断是指在某一段时间内因系统的软、硬件的故障或恶意的破坏、删除造成系统信息的受损、丢失或不可利用；窃取是指系统的信息被未经授权的访问者非法获取，造成信息不应有的泄露，使得信息的价值受到损失或者失去了存在的意义；篡改是指故意更改正确的数据，破坏了数据的真实性状态；伪造是指恶意的未经授权者，故意在系统信息中添加假信息，造

成真假信息难辨，破坏了信息的可信性。

可用性是指合法用户在需要的时候，可以正确使用所需的信息而不遭服务拒绝。系统为了控制非法访问可以采取许多安全措施，但系统不应该阻止合法用户对系统中信息的利用。信息的可用性与保密性之间存在一定的矛盾。

不可否认性是指网络信息系统应该提供适当机制保证，使发送方不能否认已发送的信息，使接收方不能否认已接收的信息。这种不可否认性质是电子商务、电子政务等领域中不可或缺的安全性要求。

1.1.2 网络信息安全的层次性

本书主要研究计算机网络环境中信息的安全问题，计算机网络环境下的信息系统可以用图 1-1 的层次结构描述。为了确保网络信息安全，必须考虑每一个层次可能的信息泄露或所受到的安全威胁。因此，本书将从以下几个层次分析网络信息安全问题：计算机硬件与环境安全、操作系统安全、计算机网络安全、数据库系统安全和应用系统安全。

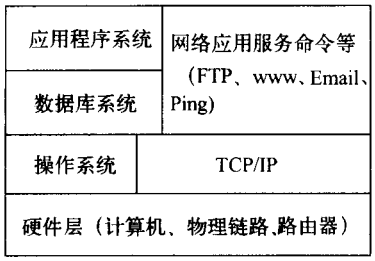

图 1-1 计算机网络信息系统的层次结构

计算机硬件安全主要介绍计算机硬件防信息泄露的各种措施，其中包括防复制技术、敏感数据的硬件隔离技术、硬件用户认证技术、防硬件电磁辐射技术和计算机运行环境安全问题。

操作系统安全主要介绍操作系统的各种安全机制，其中包括各种安全措施、访问控制和认证技术；可信操作系统的评价准则；操作系统的安全模型和可信操作系统的设计方法，其中有单级模型、多级安全性的格模型和信息流模型。操作系统的安全模型主要研究如何监管主体（用户、应用程序、进程等）集合对客体（用户信息、文件、目录、内存、设备等）集合的访问，在本书中，客体（object）也称为目标或对象。

计算机网络安全主要介绍与网络功能有关的各种安全问题，如传输信息加密、访问控制问题、用户鉴别问题、节点安全问题、信息流量控制、局域网安全问题、网络多级安全等问题，还要介绍 ISO 的网络安全框架和目前正在发展的各种网络安全增强技术。

数据库系统安全主要介绍数据库的完整性、元素的完整性、可审计性、访问控制、用户认证、可利用性、保密性等问题；还要介绍数据库安全的难点问题：敏感数据的泄漏与防范，将讨论直接泄漏与推理泄漏问题。

应用系统安全主要介绍应用系统可能受到的程序攻击、因编程不当引起敏感信息开放的问题、隐蔽信道问题、导致服务拒绝的原因、开发安全的应用系统的方法、操作系统对应用系统的安全控制与软件配置管理等内容。

1.1.3 信息对抗的阶段性

信息安全与信息对抗的方法与手段是密切相关的，熟悉信息对抗的特点是有助于信息安全的。信息的生命期是指信息从产生到消亡的整个过程，可以划分若干个阶段：信息获取，信息传输，信息储存，决策处理，信息作用，信息废弃等阶段。任何主体要想达到某种目的，比如某公司希望到某国开拓市场，那么首先应该派人到该国了解市场的需求信息，这叫

信息获取；这些信息通过无线与有线信道传输到国内公司的计算机系统中存储到数据库中，这里经历了信息传输和信息存储两个阶段，当然在数据库中还存放着该公司的生产能力、销售网络、成本核算等信息；为了决策是否到国外开拓市场，需要利用决策软件对信息进行处理和做出相应的决策；信息作用则是把决策信息返回给前端的执行机构，由执行机构实现决策的意图。信息一般都具有时效性，过了某个时效后，信息也就失去了作用，失去效用的信息应该及时废弃。信息的时效可以根据需要决定，为了留作历史资料，需要对一些信息做长时间的存储保留。

利益冲突的双方进行的信息对抗遍布信息生命期的每个阶段，而且在不同的阶段采取不同的对抗的形式。在信息获取阶段，对抗的一方需要获取对方真实完整的信息，而另一方则可以通过各种手段，如伪装、欺骗的方法使对方不能获取所需要的信息。在信息传输阶段，对抗的一方要设法让信息正确传输到目的地，而另一方则通过截获、弄假、干扰等手段妨碍信息的正确传输。在信息的存储阶段，对抗的双方围绕信息的完整性和保密性展开争斗。决策处理阶段的信息对抗体现为双方信息处理与决策支持系统之间的对抗。在信息作用阶段的信息对抗则体现为对双方信息执行机构控制权的争夺。网络黑客对信息的攻击一般都集中在信息的传输、存储和决策处理 3 个阶段中。要针对不同阶段中信息所处的不同状态，来研究不同的对抗手段。

1.2 信息安全概念与技术的发展

随着人类社会对信息的依赖程度越来越大，人们对信息的安全性越来越关注。随着应用与研究的深入，信息安全的概念与技术不断得到创新。早期在计算机网络广泛使用之前主要是开发各种信息保密技术，在 Internet 在全世界范围商业化应用之后，信息安全进入网络信息安全阶段。近几年又发展出了“信息保障（IA——Information Assurance）”的新概念。下面将介绍信息安全的各个发展阶段的主要内涵与所开发的新概念与新技术。

信息安全的最根本属性是防御性的，主要目的是防止己方信息的完整性、保密性与可用性遭到破坏。信息安全的概念与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发展的。大体可以分为单机系统的信息保密、网络信息安全和信息保障等 3 个阶段。

1.2.1 单机系统的信息保密阶段

几千年前，人类就会使用加密的办法传递信息。在 1988 年莫里斯“蠕虫”事件发生以前，信息保密技术的研究成果主要有两类：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，Hellman 在“密码学新方向”这篇开创性论文中提出来的思想，由 Rivest，Shamir，Adleman 3 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。当然，其中有

的算法是20世纪90年代提出的。

为了验证与评价计算机信息系统的安全性，在20世纪七、八十年代，研究出了一批信息系统安全模型和安全性评价准则。主要有以下几种：访问矩阵模型，这是一种最基本的访问控制模型；多级安全模型，包括军用安全模型、基于信息保密性的Bell-LaPadula信息流模型与基于信息完整性的Biba信息流模型；一些用于理论研究的抽象安全模型。如，Graham-Denning（GD）模型、对GD模型的修正模型——HRU模型和Take-Grant保护系统（TGS）等。1985年美国国防部推出了可信计算机系统评价准则TCSEC，该标准是信息安全领域中的重要创举，也为后来由英、法、德、荷四国联合提出的包含保密性、完整性和可用性概念的“信息技术安全评价准则”（ITSEC）及“信息技术安全评价通用准则”（CC for ITSEC）的制定打下了基础。

1.2.2 网络信息安全阶段

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，并于第二年成立了计算机紧急事件处理小组（CERT）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。主要有以下一些：

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，并提供相应的解决方案。

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的堡垒主机，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一类系统，IDS一般也同时具备告警、审计和简单的防御功能。

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，目的是防止内部网络受到攻击，保护内部网络的信息安全。

1.2.3 信息保障阶段

信息保障的概念与思想是美国国防部在20世纪90年代末提出来的，该思想的基本完善是在2000年的下半年。因此信息保障阶段可以大致认为是从21世纪初开始的。下面介绍信息保障阶段的主要内容。

1. 信息保障框架

（1）信息保障的概念

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正常运转，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），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。

1998年5月美国公布了由国家安全局NSA起草的1.0版本《信息保障技术框架》IATF，在1999年8月31日IATF论坛发布了IATF2.0版本，2000年9月22日又推出了IATF3.0版本。遵循IATF3.0中定义的原则，就可以对信息基础设施做到多重保护。这称为“纵深防卫策略”DiD（Defense-in-Depth Strategy），其内涵已经超出了传统的信息安全保密，而是保护（Protection）、检测（Detection）、反应（Reaction）、恢复（Restore）的有机结合，这就是所谓的PDRR模型（如图1-2所示）。根据PDRR模型的含义，信息保障阶段不仅包含安全防护的概念，更重要的是增加了主动的和积极的防御观念。

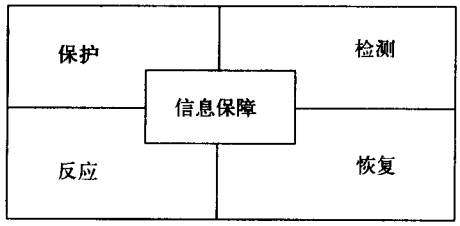

图1-2 PDRR模型

信息保障（IA）依赖于人、技术及运作三者去完成使命（任务），还需要掌握技术与信息基础设施。要获得鲁棒（即健壮）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。IATF主要包含：说明IATF的目的与作用（帮助用户确定信息安全需求和实现他们的需求）；说明信息基础设施及其边界、IA框架的范围及威胁的分类和纵深防御策略（DiD——Depth in Defense）；DiD的深入介绍；信息系统的安全工程过程（ISSE）的主要内容；各种网络威胁与攻击的反制技术或反措施；信息基础设施、计算环境与飞地的防御；信息基础设施的支撑（如密钥管理/公钥管理，KMI/PKI）、检测与响应以及战术环境下的信息保障问题。下面简要介绍IA框架的区域划分和纵深防御的目标、ISSE的主要内容、和信息安全技术的反制措施。

信息基础设施的要素包括网络连接设施和各单位内部包括局域网在内的计算设施。网络连接设施包括由传输服务提供商TSP提供专用网（其中还可能包括密网）、公众网（Internet）和通过Internet服务提供商ISP提供信息服务的公用电话网与移动电话网（参见图1-3）。

IA框架是建筑在上述信息基础设施之上的。IA划分为四类区域：

1）本地计算环境：包括服务器、客户机，以及安装在它们上面的应用软件。应用软件包括那些提供调度、时间管理、打印、字处理和目录服务等等功能的软件，为用户提供信息处理的平台。

2）飞地边界：是指围绕本地计算环境的边界。受控于单个的安全策略，并通过局域网互联的本地计算设备的一个集合称为一个“飞地”（enclave）。由于针对不同类型和不同级别的信息的安全策略是不同的，所以一个单个的物理设施会有多个飞地。对一个飞地内设备的本地和远程访问必须满足该飞地的安全策略。飞地分为与内部网连接的内部飞地、与专用网连接的专用飞地和与Internet连接的公众飞地。

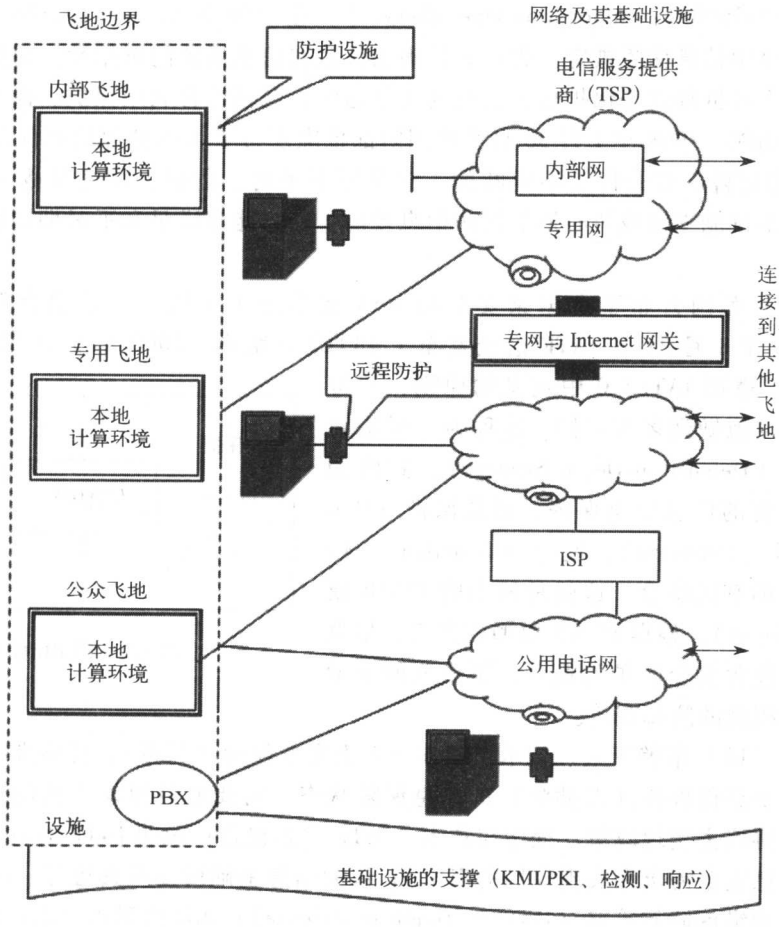

图 1-3　IA 框架中的区域与防御

3）网络及其基础设施：提供了飞地之间的连接能力，包括可运作区域网络（Operational Area Networks，OAN）、城域网（MAN）、校园网（CAN）和局域网（LAN），其中也包括专用网、Internet 和公用电话网及它们的基础设施。

4）基础设施的支撑：提供了能应用信息保障机制的基础设施。支撑基础设施为网络、终端用户工作站、Web 服务器、文件服务器等提供了安全服务。在 IATF 中，支撑基础设施主要包括两个方面，一是密钥管理基础设施（KMI），包括公开密钥基础设施（PKI）；二是检测与响应基础设施。

（2）纵深防御（Defense-in-Depth）

IATF 的一个突出的贡献就是提出了纵深防御的概念。纵深防御是一种安全策略，用来获得高效的信息保障态势。纵深防御策略的基本原则可以适用于任何的信息系统，而不管它是属于何种机构的。从本质上说，信息保障依赖于人、技术及操作三者去完成任务并掌握技术及信息基础设施，即人在技术的支持下去执行操作从而来对信息系统进行保障。

纵深防御的策略包括对人、技术和操作三种因素的要求与控制。

1）人的因素：包括培训、了解、物理安全、人员安全、系统安全和行政管理等内容。

2）技术因素：包括纵深防御技术、框架的四个领域、安全准则、IT/IA 采购、风险评估和确证与认可。

3）操作因素：包括评估、监视、入侵检测、告警、应急响应和系统恢复。

纵深防御的目标就是要解决 IA 框架中四个领域中目标的防御问题。首先根据用户计算信息安全性等级的高低，将用户计算环境划分为绝密飞地、机密飞地、秘密飞地、无密飞地和公共飞地非敏感区等区域，然后分别为这些飞地提供相应安全等级的网络信道。对于飞地的边界要增设防卫，如防火墙、路由器过滤等。对于远程用户需要采取远程接入防护措施，如通信服务的安全性和加密等。在整个基础设施中要采用密钥管理/公钥管理（KMI/PKI），要坚持检测，以便及时发现入侵，并能及时进行应急响应与处理，确保信息基础设施的随时安全。

2. 信息系统安全工程过程（ISSE）

ISSE 主要告知人们如何根据系统工程的原则构建安全信息系统的方法、步骤与任务。系统工程过程主要包括以下步骤与任务：

（1）发现需求

包括以下任务：

1）使命/业务的描述。使命是指一个单位所担负的特定任务，由任务可以划分为功能。

2）有关政策方面的考虑。如国家或军队的信息管理要求；原始与历史资源的管理要求；与 C3I 系统的兼容性、互操作与集成要求等。

（2）系统功能的定义

1）目标：确定系统的功能及与外部的接口，并转换成工程图的定义、接口与系统的边界。

2）系统的上下文环境：包括系统的物理及逻辑边界、连接到系统的输入和输出的特点，还应标明支持用户完成使命所需的信息处理类型（交互通信、广播通信、信息存储、一般访问、受限访问等）。

3）要求：描述任务、行动及完成系统需求的活动等。

（3）系统的设计

1）功能分配。

2）概要设计。

3）详细设计。

（4）系统的实现

1）获得一切必要的资源，包括通过采办手段。

2）按照需求构建系统。

3）系统测试。

4）评估性能。

（5）ISSE 过程

ISSE 作为上述系统工程过程的一个子过程，其重点是针对信息保护方面的需求，从理论上讲它是与上述系统工程平行出现的，分布在各个阶段。ISSE 的活动包括：

1）描述信息保护的需求。

2）基于前述系统工程过程，形成信息安全方面的要求（安全要适度）。

3）根据这些要求构建功能性的信息安全体系结构。