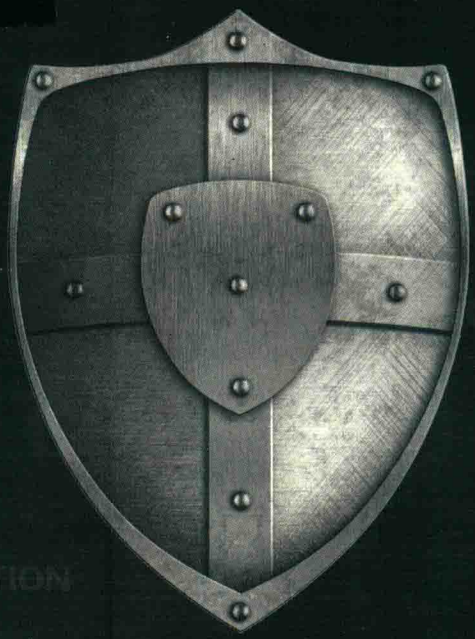
国家

21世纪高等教育信息安全系列规划教材



信息安全工程与实践

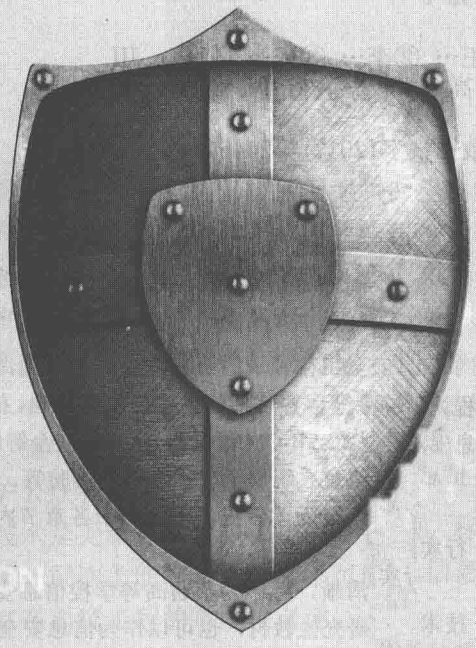
王瑞锦◎主编

李冬芬 朱国斌 张凤荔◎编著

中国工信出版集团

人民邮电出版社
POSTS & TELECOM PRESS

21世纪高等教育信息安全系列规划教材



信息安全工程与实践

王瑞锦◎主编
李冬芬 朱国斌 张凤荔◎编著

人民邮电出版社
北京

图书在版编目（CIP）数据

信息安全工程与实践 / 王瑞锦主编 ; 李冬芬, 朱国斌, 张凤荔编著. -- 北京 : 人民邮电出版社, 2017.8
21世纪高等教育信息安全系列规划教材
ISBN 978-7-115-46652-5

Ⅰ. ①信… Ⅱ. ①王… ②李… ③朱… ④张… Ⅲ. ①信息安全－安全工程－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2017)第244515号

内 容 提 要

本书全面、系统地阐述了信息安全工程领域的经典理论体系结构，辅以典型工程案例，为读者展示了成熟的分析方法及解决方案。全书内容包括信息安全工程基础、信息系统安全工程过程（ISSE工程）、信息安全工程能力成熟度模型（SSE-CMM 模型）、信息安全等级保护、信息安全风险评估、信息安全管理基础、信息安全策略、信息系统安全工程案例及实验等。

本书的结尾，围绕全书的知识脉络，为读者提供了紧贴于各章节内容的实验任务，方便读者进行实践。

本书难易适中，内容充实、层次清晰，可作为普通高等学校信息安全、软件工程、计算机科学技术、网络空间安全等专业本科生及研究生教材，也可以作为信息安全工程师的参考手册。

◆ 主　　编　王瑞锦
编　　著　李冬芬　朱国斌　张凤荔
责任编辑　邹文波
责任印制　陈　犇

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京市艺辉印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：16.5　　2017 年 8 月第 1 版
字数：398 千字　　2017 年 8 月北京第 1 次印刷

定价：49.80 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

前　言

随着科学技术的飞速发展，人类社会发生了翻天覆地的变化，信息技术作为科学技术的一个重要分支，在人类的生产、生活中扮演者越来越重要的角色。相关数据显示，2016 年，我国电子商务交易市场规模居全球第一，电子商务交易额超过 20 万亿元，占社会消费品零售总额的比重超过 10%。信息产业已经渗透到人类生活的方方面面，以信息技术为基础的信息产业已经成为世界经济的重要支柱产业。但随之而来的是一次次骇人听闻的信息泄露事件，个人信息就如同被包裹在泡沫中，一戳就破。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，维护国家安全已经刻不容缓。

信息系统安全问题单凭技术是无法得到彻底解决的。它的解决涉及政策法规、管理、标准、技术等方方面面，任何单一层次上的安全措施都不可能提供真正的全方位的安全。信息系统安全问题的解决更应该站在系统工程的角度来考虑。

“三分技术、七分管理”，安全问题的产生很大程度上是由于对信息资产所面临威胁的严重性认识不足，缺乏明确的信息安全方针和完整的信息安全管理制度，相应的管理措施还不到位。信息安全管理作为信息安全保障体系中重要的一环，应该得到广泛的关注。

本书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的相关标准和规范，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。

全书共分为 8 章，按照信息安全工程理论与技术的脉络逐步展开。第 1 章信息安全工程基础，描述了信息安全问题产生的根源，并依此提出了信息安全工程的概念。第 2 章信息系统安全工程过程，详细讲解了安全需求的挖掘、定义、设计、实施和评估过程，并辅以相关实例系统地介绍了信息系统安全工程。第 3 章信息安全工程能力成熟度模型，引入能力成熟度模型对组织的工程能力进行评估，详细分析了能力成熟度模型的体系结构及其应用。第 4 章信息安全等级保护，系统性地阐述了我国信息安全等级保护体系建设，并给出了信息系统安全定级方法。第 5 章信息安全风险评估，全面解释了信息风险评估方法，同时讲解了相关风险评估软件的使用方法。第 6 章信息安全管理基础，在概述信息安全管理标准的同时，重点介绍信息安全体系过程。通过具体实例对信息安全体系准备、建立、实施和运行、监视和评审、保持和改进、认证过程进行了具体的分析。第 7 章信息安全策略，对常见的信息安全问题进行了解释，同时针对这些问题，提出了可行性防护方案。第 8 章信息系统安全工程案例，是信息安全工程的实践部分，在了解信息安全工程前沿技术的同时，对前 7 章所涉

及的理论框架进行了回顾。附录展示紧贴各章内容的实验任务，旨在增强读者实践的能力，这也是本书设计的核心理念。

本书难易适中、内容充实、层次清晰，可作为普通高等学校信息安全、软件工程、网络工程、物联网工程等专业本科生及研究生教材，也可以作为信息安全工程师的参考手册。

本书由电子科技大学信息与软件工程学院牵头，与成都理工大学网络安全学院合作编写。参加本书编写工作的有：王瑞锦、李冬芬、朱国斌、张凤荔。具体编写分工如下：王瑞锦编写第 1～3 章，张凤荔编写第 4 章，朱国斌编写第 5 章，李冬芬编写第 6～8 章。张雪岩、刘崛雄、唐晨、魏楷等几位研究生参与了本书部分章节的资料收集和整理，李悦、黄俊钦本科生对书稿资料收集和插图做了不少工作，诚挚感谢他们对本书所做的贡献。

信息安全工程与实践是以工程实践的角度看待信息安全，是信息安全应用发展的新趋势，本书初步总结了此领域的理论及技术，以期有益于读者。

编者

目 录

▶▶▶ 第 1 章

信息安全工程基础

当今世界已经进入了信息时代，在商场，谁掌握了信息就等于掌握了商机；在战场，控制了信息权就等于控制了战场。随着信息地位的越发重要，信息安全的作用也越发凸显。信息安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改和泄露，系统能连续可靠正常地运行，信息服务不中断。信息安全涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多个领域。

信息安全工程是从工程的角度将概念、原理、技术和方法应用于研究、开发、实施与维护信息系统安全的过程。通过整个信息安全工程过程，我们可以建立起能够面对错误、攻击和灾难的可靠信息系统。

本章旨在对信息安全工程进行整体的介绍。在 1.1 节中，我们将对信息的本质进行概述，从信息论的观点对信息安全的重要性进行阐述，介绍信息安全发展的几个重要时期以及各个时期的特点，并从四个层面上介绍信息安全的具体目标。1.2 节在对信息安全保障这个重要的概念进行解释的同时，我们将对信息安全问题的产生原因进行阐述，并从三方面对信息安全保障模型进行叙述。接着，对 IATF 保障框架进行详细介绍并对信息安全保障体系建设进行相关说明。在 1.3 节，我们将对信息安全工程做一个整体的概述，包括其基本概念、发展历程。最后对本书所涉及的理论技术作一个简要的概述。

【学习目标】

- 了解信息安全的发展和现状，学习信息安全的目标。
- 对信息安全保障进行深入学习，包括模型和框架。
- 对信息安全工程进行初步学习，掌握概念、实施方法和技术支持。

1.1 信息安全概述

“信息是能够用来消除随机不确定性的东西”，这是信息论创始人克劳德·香农在 1948 年提出的对信息的数学定义。信息是对客观世界中各种事物的运动状态和变化的反映，是客观事物之间相互联系和相互作用的表征，表现的是客观事物运动状态和变化的实质内容。

人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。在信息时代，信息产业成为世界第一大产业。信息就像水、电、石油一样，已经成为一种基础资源。信息和信息技术改变着人们的生活和工作方式。离开计算机、电视和手机等电子信息设备，人们将无法正常生活和工作。因此可以说，在信息时代人们生存在物理世界、人类社会和信息空间组成的三维世界中。

早在 1982 年，加拿大作家威廉·吉布森在其短篇科幻小说《燃烧的铬》中创造了 Cyberspace

一词，意指由计算机创建的虚拟信息空间。此后，随着信息技术的快速发展和互联网的广泛应用，Cyberspace 的概念得到不断丰富和演化。目前，国内外对 Cyberspace 还没有统一的定义。我们认为，它是信息时代人们赖以生存的信息环境，是所有信息系统的集合。因此把 Cyberspace 翻译成信息空间或网络空间是比较好的。

人身安全是人对其生存环境的基本要求，即要确保人身免受其生存环境的危害。因此，哪里有人那里就存在人身安全问题，人身安全是人的影子。同样，信息安全是信息对其生存环境的基本要求，即要确保信息免受其生存环境的危害。因此，哪里有信息那里就存在信息安全问题，信息安全是信息的影子。

根据信息论的基本观点，系统是载体，信息是内涵。因此，网络空间安全的核心内涵仍是信息安全，没有信息安全就没有网络空间安全。

1.1.1 信息安全的发展

提及信息安全这一词，很多人会联想到 IT、计算机、网络等词语，而信息安全的发展阶段大致可以分为以下 4 个时期。

第一个时期为 20 世纪 40～70 年代。其主要标志是 1949 年香农发表的《保密系统的通信理论》。在此阶段中，通信技术不发达，人们主要使用电话、传真等进行通信，其主要的安全问题为通信过程中的信息交换，其主要的解决方法是通过密码（主要是序列密码）解决通信安全的保密问题，所以这一阶段可以称为“通信安全时期”。这一阶段人们的研究重点在于探究各种复杂程度的密码来防止信息被窃取，而这种复杂程度限于当时的计算能力。

第二时期为 20 世纪 70～80 年代的“计算机安全时期”。这一时期半导体和集成电路技术得到飞速发展，因而推动了计算机软硬件的发展。同时网络技术的发展使数据传输可以通过计算机网络来完成，人们关注的焦点扩展为网络数据传输、处理和存储的保密性、可用性和完整性，主要保证动态信息不被窃取、解密或篡改，从而让读取信息的人能够看到准确无误的信息。1977 年美国国家标准局（NBS）公布的国家数据加密标准（DES）和 1983 年美国国防部公布的可信计算机系统评价准则（Trusted Computer System Evaluation Criteria，TCSEC，俗称橘皮书）标志着信息安全由简单的通信问题转变为信息系统安全问题。

第三时期是从 20 世纪 90 年代开始兴起的网络时代。这一时期被称为“信息系统安全时期”。随着互联网技术的飞速发展，网络规模的扩大化以及网络的开放性，信息无论是企业内部还是外部都得到了极大的开放，而由此产生的信息安全问题跨越了时间和空间。信息安全的焦点已经从传统的保密性、完整性和可用性 3 个原则衍生为诸如可控性、抗抵赖性、真实性等其他的原则和目标。这一阶段的安全威胁主要有网络入侵、病毒破坏、信息对抗等，其重点在于保护比“数据”更精炼的“信息”，以确保信息在存储、处理和传输过程中免受偶然或恶意的非法泄密、转移或破坏，安全措施主要有防火墙、防病毒、漏洞扫描、入侵检测、PKI、VPN 等。

第四时期是从 21 世纪开始的“信息安全保障时期”。这一时期的主要标志是 1998 年美国国家安全局（NSA）提出的《信息保障技术框架》（IATF）。信息安全保障这一理念，不仅仅是从系统漏洞方面考虑，还要从业务的生命周期、业务流程来进行分析，其核心思想是综合技术、管理、过程、人员等，在不同的阶段进行安全保障。通过把安全管理和技术防御相结

合，如今的防护措施已经不再是被动地保护自己，而是主动地防御攻击，也就是说安全保障理念已经从风险承受模式走向安全保障模式，信息安全阶段已经转变为从整体角度考虑体系建设的信息安全保障时代。

第五时期是从 2009 年至今。这一时期被称为 Cyber Security/Information Assurance（CS/IA），也就是网络空间安全和信息安全保障相结合。2009 年 10 月美国正式成立网络作战司令部，在美国的带动下，世界各国的信息安全政策、技术和实践等方面都发生着重大的变革，各国在信息安全方面都达成一个共识，那就是将网络安全提升到国家安全的重要程度。其核心思想是：从传统防御的信息保障（IA），发展到“威慑”为主的防御、攻击和情报三位一体的信息保障/网络空间安全（IA/CS），即网络防御（Defense）、网络攻击（Offense）和网络利用（Exploitation）。

当前，一方面信息技术与产业的空前繁荣，另一方面危害信息安全的事件不断发生。敌对势力的破坏、黑客攻击、恶意软件侵扰、利用计算机犯罪、隐私泄露等，对信息安全构成了极大威胁。

黑客攻击已经成为经常性、多发性的事件。全国性或国际性的大型活动，都可能遭到大量的黑客的攻击。计算机病毒等恶意代码是黑客的主要攻击武器。目前，计算机病毒有几万种，而且还在继续增加。追求经济和政治利益已经成为研制和使用计算机病毒的新目的。恶意软件的开发、生产、销售，形成了一条地下产业链。

利用计算机进行经济犯罪带来的影响已经远超普通经济犯罪。目前网上银行诈骗和电信诈骗等成为案件的高发区，钓鱼银行网站、伪造银行卡、网络诈骗、电话诈骗等，给人民群众造成了严重的经济损失。

网络上仍存在相当多的有害内容。垃圾邮件、黄赌毒内容、伪科学的内容、政治上不健康的内容时有发现，网络环境还待进一步规范、治理。宣扬网络精神文明成为国家的一项重要任务。

综上所述，网络空间安全的形势是严峻的。

1.1.2 信息安全的目标

信息论的基本观点告诉我们，信息不能脱离它的载体而孤立存在，因此我们不能脱离信息系统而孤立地谈论信息安全。也就是说，每当我们谈论信息安全时，总是不可避免地要谈论信息系统的安全。这是因为，如果信息系统的安全受到危害，则必然会危害到存在于信息系统之中的信息的安全。据此，我们应当从信息系统的角度来全面考虑信息安全的内涵。

信息安全的总体目标是保护信息免受各种威胁的损害，以确保业务连续性，业务风险最小化，投资回报和商业机遇最大化。

从纵向来看，信息安全主要包括以下 4 个层面：设备安全、数据安全、行为安全以及内容安全。其中数据安全即是传统的信息安全。

1. 设备安全

信息系统设备（硬设备和软设备）的安全是信息系统安全的首要问题。这里包括三个侧面。

（1）设备的稳定性：保证设备在一定时间内不出故障的概率。

（2）设备的可靠性：保证设备能在一定时间内正确执行任务的概率。

（3）设备的可用性：设备随时可以正确使用的概率。

2. 数据安全

数据安全是指采取措施确保数据免受未授权的泄露、篡改和毁坏。传统的信息安全强调信息（数据）本身的安全属性。数据安全主要包含以下 3 点。

（1）保密性：数据不被未授权者知晓的属性。

（2）完整性：保证数据正确的、真实的、未被篡改的、完整无缺的属性。

（3）可用性：数据可以随时正常使用的属性。

除了上述 3 点之外，数据安全的基本要求还延伸至其他方面，比如下述几点。

（1）真实性：对信息的来源进行判断，能对伪造来源的信息予以鉴别。通过保证信息的真实性来防止被虚假信息欺骗。

（2）不可抵赖性：建立有效的责任机制，防止用户否认其行为，这一点在电子商务中极其重要。

（3）可控制性：对信息的传播及内容具有控制能力。管理机构对危害国家的来往信息、使用加密手段从事非法的通信活动等进行监视审计，从而达到对信息的控制。

3. 行为安全

行为安全是从主体行为的过程和结果来考察是否会危害信息安全，或者说是否能够确保信息安全。从行为安全的角度来分析和确保信息安全，符合哲学上实践是检验真理唯一标准的基本原理。

（1）行为的秘密性：行为的过程和结果不能危害数据的秘密性，必要时行为的过程和结果也应是保密的。

（2）行为的完整性：行为的过程和结果不能危害数据的完整性，行为的过程和结果是预期的。

（3）行为的可控性：当行为过程偏离预期时，能够发现、控制或纠正。

4. 内容安全

内容安全是信息安全在政治、法律、道德层次上的要求，是语义层次的安全。

（1）信息内容在政治上是健康的。

（2）信息内容在法律上符合国家法律法规。

（3）信息内容符合中华民族优良的道德规范。

根据上面的分析，要确保信息系统的安全，就必须确保信息系统的设备安全、数据安全、行为安全和内容安全。信息系统的硬件系统安全和操作系统安全是信息系统安全的基础，密码和网络安全等技术是信息系统安全的关键技术。确保信息系统安全是一个系统工程，只有从信息系统的硬件和软件的底层做起，从整体上综合采取措施，才能有效地确保信息系统的安全。

1.2 信息安全保障

在本节中，我们首先将介绍信息安全问题产生的原因，包括内在和外在因素。接着我们将重点对信息安全保障进行全方位的介绍，对其中信息安全保障模型，我们将从保障要素、生命周期和安全特征 3 个方面进行说明；对 IATF 框架，我们将对它的整体框架以及信息保障技术进行叙述。最后，我们将对国内外的信息安全保障体系建设进行详细介绍。

1.2.1 信息安全问题的产生

从 20 世纪 90 年代开始，随着互联网技术飞速发展至今，人类已经步入了大数据时代。大数据在健康医疗、金融商务、物流快递、城市管理、社会治理、生产制造等领域都具有无穷的潜力，其带来的革命性进步令人神往。

大数据应用的场景越来越多、越来越深入。例如，根据关键基础设施的数据、特定行业的基础数据以及生产数据，能够分析出一个国家的重要战略情报，直接关系到国家安全。可以说，数据越来越值钱。因此也成为违法犯罪分子的重点关注目标。全球各式各样的数据安全事件层出不穷，包括直接盗取数据进行倒卖、用数据构建精准诈骗活动，甚至对用户数据进行加密，然后勒索赎金。数据安全正在成为全世界的热点安全问题，从当今人类社会发展来看，如果数据安全问题失控，必然会影响全社会对数字经济的信心，阻碍人类社会的进步。

从信息安全的角度来看，信息安全问题产生的根源主要分为内在因素和外在因素。

内在因素主要是信息系统的复杂性，其复杂性又可以分为过程复杂和结构复杂。对过程复杂性而言，从理论上来看，在程序和数据上存在“不确定性”，不论是从软件还是硬件上都可能导致未知的错误；从设计的角度看，在设计时所考虑的优先级中，相对于易用性、代码大小、执行程度等因素，安全性往往被放在次要位置；在实现上来说，软件本身总存在 Bug；而在系统的使用上，由于人的操作失误造成的相关信息的丢失或修改同样会导致安全问题；最后在系统维护的过程中，由于安全设计和实现的不完整或者管理的不完善也会给不法分子提供攻击的机会。结构复杂性主要指系统涉及各方面的协调运行，比如网络中的其他系统和资源，开放的网络端口，远程的用户使用，公共信息服务等。

外在因素主要指人为威胁和自然威胁。人为威胁有情报威胁，比如间谍搜集国家的政治、军事、经济信息，针对国家进行非法活动；恐怖分子破坏公共秩序，散布恐怖信息，制造混乱，发动政变；犯罪团伙实施报复，实现经济目的，破坏社会制度；商业间谍进行非法窃取；黑客进行网上盗窃、恐吓、诈骗等。而自然威胁则指的是恶劣的自然环境所导致的系统瘫痪，信息无法传递、丢失等，这些恶劣环境包括雷雨天、冰雪天、洪水、台风等自然灾害。

1.2.2 信息安全保障模型

信息安全保障是在信息系统的整个生命周期中，通过对信息系统的风险分析，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。图 1-1 描述了信息系统安全保障模型。

信息系统安全保障模型包括保障要素、生命周期和安全特征这 3 个方面。

1. 保障要素

保障要素强调信息安全技术体系、信息安全工程过程、信息安全管理体系和高素质的人员队伍。

（1）信息安全技术体系

完善的信息安全技术体系是实现信息保障的重要手段，信息安全保障中各种安全服务就是通过各种防御技术来体现的，如图 1-2 所示。该图展现了部分保障信息安全的核心技术。在使用路由器时更改默认的系统口令；使用防火墙的安全策略实现严格的访问控制，以允许

必要的流量通过防火墙，阻止到 Internet 的未授权的访问，保证网络资源不被非法使用和非法访问；通过入侵检测技术实时监控网络传输，自动检测可疑行为，分析来自网络外部入侵信号和系统内部的非法活动，在系统受到危害前发出警告，对攻击做出实时的响应，并提供补救措施，最大程度地保障系统安全；在系统内部使用反病毒产品防止计算机病毒对系统的传染和破坏，利用计算机 CPU 内嵌的防病毒技术来防范大部分针对缓冲区溢出漏洞的攻击；通过漏洞扫描等手段对本地计算机系统的安全脆弱性进行检测，发现可能被利用的漏洞，同时通过补丁管理对相关的漏洞进行修复；对系统中重要的数据文件进行加密以防止信息被窃取；使用审计系统对一个信息系统的运行状况进行检查与评价，以判断信息系统是否能够保证资产的安全、数据的完整并有效利用组织的资源。

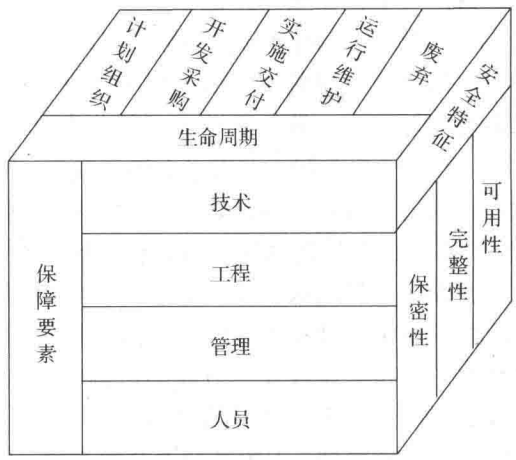


图 1-1　信息系统安全保障模型

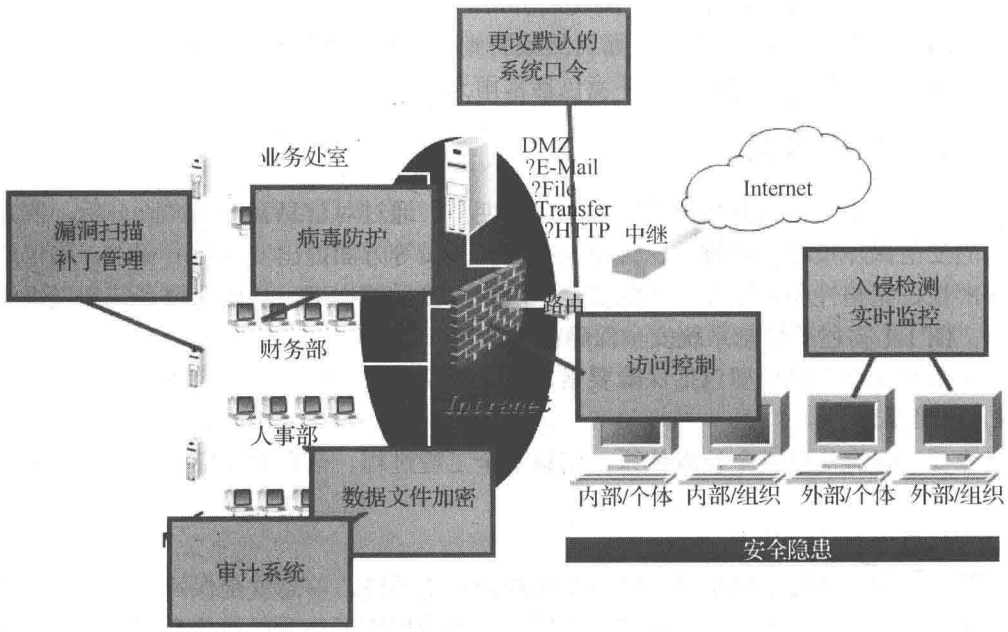


图 1-2　保障信息安全的核心技术

（2）信息安全工程过程

信息安全是一个复杂的系统工程，因此解决安全问题应该从工程学、方法论的角度来考虑，通过一系列的工程过程来实现信息安全保障。比如通过风险评估来对采用的安全策略和规章制度进行评审，发现不符合项；采用模拟攻击的形式对目标可能存在的安全漏洞进行检查，从而确定存在的安全隐患和风险级别；通过安全需求分析来发掘出系统的安全需求，时刻根据系统的变化进行同步发展；根据实际情况来进行安全体系设计来确保安全体系的可靠性、可行性、完备性和可扩展性；制定相应的安全策略来调动、协调和指挥各方面的力量，共同维护信息系统的安全等。

（3）信息安全管理体系

随着组织机构的使命越来越依赖于信息系统，信息系统也越来越成为组织机构生存和发展的关键因素。信息系统的安全也成为了组织风险的一部分，为了保障组织机构能够完成其使命，必须为组织机构制定相应的管理体系来防范各种安全风险，如图 1-3 所示。国家、机构和相关业务所制定的策略、规范和标准，组织机构本身的使命要求以及相应的安全风险都推动着组织管理体系的建设。在管理体系的建设过程中，形成相应的策略体系，比如风险管理、业务持续性管理、应急响应管理、意识培训和教育等。通过相关的管理和培训对系统形成风险评估，最后将风险评估融入到整个安全管理的生命周期当中。

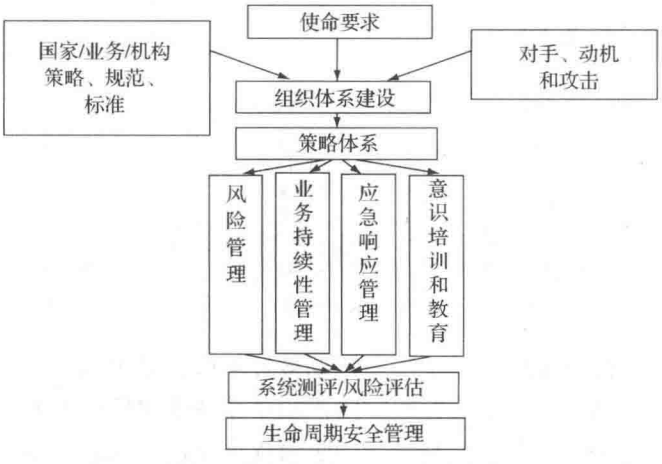


图 1-3　信息安全保障管理体系建设

（4）高素质的人员队伍

信息安全对抗归根结底是人与人的对抗，因此建立高素质的人员队伍对于信息安全尤为重要。保障信息安全不仅需要专业的信息技术人员，还需要提高信息系统普通使用者的安全意识，加强个人防范，如图 1-4 所示。

① 信息安全专业人员，比如注册信息安全专业人员（CISP），他们对信息安全相关的岗位和职责要十分清楚。由于从开始的计划组织到最后的废弃，整个过程他们都要进行相关的安全工作，因此他们需要通过培训学习信息安全的生命周期过程。

② 信息安全从业人员，比如注册信息安全员（CISM），要通过培训学习相关的安全的基础知识和安全文化以便进行相关工作。