普通高等教育“十一五”国家级规划教材
21世纪高等教育信息安全系列规划教材

“十三五”
国家重点图书出版规划项目

信息安全管理

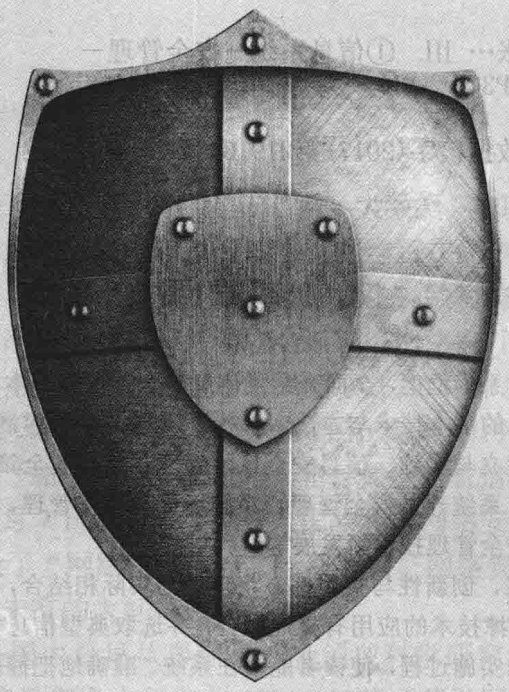
（第2版）

张红旗 杨英杰 唐慧林 常德显◎编著

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

普通高等教育“十一五”
21世纪高等教育信息安

“十三五”
国家重点图书出版规划项目



信息安全管理

（第2版）

张红旗 杨英杰 唐慧林 常德显◎编著

人 民 邮 电 出 版 社
北 京

图书在版编目（CIP）数据

信息安全管理 / 张红旗等编著. -- 2版. -- 北京 : 人民邮电出版社, 2017.9
21世纪高等教育信息安全系列规划教材
ISBN 978-7-115-46807-9

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息系统－安全管理－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2017)第219134号

内 容 提 要

本书以信息安全管理体系为框架，全面介绍了信息安全管理的基本概念、主要内容和相关任务，以及构建信息安全管理体系的基本技术与方法。全书共分 12 章，内容涵盖了信息安全管理的基本内涵、信息安全管理体系的建立与实施、信息安全风险管理、信息安全策略管理、组织与人员安全管理、环境与实体安全管理、系统开发安全管理、系统运行与操作管理、安全监测与舆情分析、应急响应处置管理，以及信息安全管理技术新发展等。

本书注重知识的系统性、创新性与实用性，将理论与实际相结合，在全面介绍信息安全管理理论的基础上，将管理与其支撑技术的应用有机地融合，并选取典型信息安全管理实施案例进行分析，充分阐释了信息安全管理的实施过程，使读者能够在系统、准确地把握信息安全管理思想的基础上，正确、有效地运用信息安全管理的方法和技术分析、解决实际问题。

本书可作为网络空间安全相关专业的本科生及研究生教材，或信息管理与信息系统专业、计算机相关专业的参考书，也可作为信息化管理人员、安全管理人员、网络与信息系统管理人员的参考手册和培训教材。

◆ 编　　著　张红旗　杨英杰　唐慧林　常德显
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
三河市中晟雅豪印务有限公司印刷

◆ 开本：787×1092　1/16
印张：16.5　　2017 年 9 月第 2 版
字数：396 千字　　2017 年 9 月河北第 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

安徽大学图书馆 藏书 www.lib.ahu.edu.cn

前言

随着网络和通信技术的飞速发展，特别是云计算、大数据、物联网等新技术的逐步应用，网络空间已成为国家关键信息基础设施和重要战略资源，正在深刻改变着社会的生产形态和人们的生活方式。与此同时，网络空间安全事件频繁发生，敌对势力的破坏、黑客入侵、计算机犯罪、恶意代码侵扰等严重影响了网络的安全运转，网络空间安全形势异常严峻。

我国政府高度重视网络空间安全。习近平总书记早在2014年就明确指出："没有网络安全就没有国家安全，没有信息化就没有现代化"，在2016年4月19日召开的网络安全和信息化工作座谈会上进一步要求"加快网络立法进程，完善依法监管措施，化解网络风险"。全国人大常委会也于2016年11月7日发布了《中华人民共和国网络安全法》。此外，经国务院学位委员会批准，2015年增设了"网络空间安全"一级学科。网络安全技术创新发展与网络空间安全人才培养迎来了前所未有的大好机遇。

解放军信息工程大学是国内最早从事信息安全领域科学研究和人才培养的军事院校，2000年创建了军内第一个信息安全本科专业，2016年获评首批网络空间安全一级学科博士学位授予点，是中央网信办批准的5个网络安全人才培养基地之一。为适应信息安全人才培养的需要，2007年学校组织编写出版了《信息安全管理》教材，被国内许多高校采用，并得到了广大读者的厚爱。为满足读者需求，我们课程组结合近年来的教学实践经验，并参考信息安全管理领域的最新研究成果，在原书的基础上进行了修订、改版，出版了《信息安全管理（第2版）》。

《信息安全管理（第2版）》较之第1版，最主要的特点和变化如下。

（1）进一步提升了知识的完整性和系统性。第1版编写出版后，国际标准化组织出版了ISO 27000系列信息安全管理标准，国家标准化委员会出版了等级保护系列标准，结合以上相关标准，第2版对信息安全管理知识体系进行了充实和优化。

（2）增加了信息安全管理技术方面知识的比重。在信息安全管理的各个管理环节和过程中离不开技术的支撑，例如，信息安全风险评估、信息安全策略管理、信息安全监察与态势感知、信息安全事件应急处置等。第2版在第1版的基础上进行了管理技术梳理与补充，将技术与相关信息安全管理环节和过程有机结合，从而使得信息安全管理理论与技术形成一个有机体。

（3）补充了信息安全管理技术实践性内容。信息安全管理十分注重实践性，为了便于读者掌握，在第2版中我们引入了部分信息安全管理技术实验和实践教学内容。

（4）充实、丰富了信息安全管理案例。为了便于读者理解信息安全管理知识体系，在第2版中我们针对难以理解的信息安全管理知识环节，充实了实践案例，从而使得抽象内容更加通俗易懂。

《信息安全管理（第2版）》以信息安全管理体系为框架，全面介绍了信息安全管理的基本概念、主要内容和相关任务，以及构建信息安全管理体系的基本技术与方法。期望读者通过阅读本书，能够对构建信息安全管理体系的基本理论、技术和方法有一个整体和系统化的认识和理解，提升信息安全管理体系设计与构建的实践能力。

本书共12章，由解放军信息工程大学张红旗教授牵头，信息安全管理课程组共同编写，其中第1、2章由张红旗、杨英杰和刘育楠编写，第3、10章由唐慧林、杨英杰编写，第4、5、6、8章由杨英杰、王义功、刘江编写，第7、9、11章由常德显、汪永伟、胡浩、雷程、刘艺编写，第12章及附录由祝宁、唐慧林编写，全书由张红旗、杨英杰、唐慧林、常德显负责统稿。

在本书编写过程中，编者参考引用了大量的相关文献，在此谨向这些文献的作者表示衷心的感谢。

衷心感谢给予编者指导、支持和帮助的领导、专家和同行。

信息安全学科内容广泛，发展迅速，信息安全管理及相关内容也在不断更新。由于编者水平有限，书中难免存在不足和错误之处，敬请读者批评指正。

编者

2017年6月30日

试读结束：需要全本请在线购买： www.ertongbook.com

目　录

试读结束：需要全本请在线购买： www.ertongbook.com

▶▶▶ 第 1 章

信息安全管理概述

人类正进入信息化社会，社会发展对信息资源的依赖程度越来越高。从人们的日常生活、组织运作，到国家管理，信息资源都是不可或缺的重要资源，没有各种信息的支持，现代社会将无法存在和发展。而由于环境的开放和信息系统自身的缺陷，信息资源面临着来自内部和外部两个方面的威胁。随着信息技术和信息安全的发展，人们不断意识到，必须从技术和管理两个方面采取安全措施，才能保证信息系统和信息资源的安全。

本章介绍信息安全管理的产生背景、信息安全管理的内涵、国内外信息安全管理现状，以及信息安全管理相关标准规范。

本章重点：信息安全管理的内涵、信息安全管理相关标准。

本章难点：信息安全管理的内涵。

1.1 信息安全管理的产生背景

信息安全管理是随着信息和信息安全的发展而发展起来的。在信息社会中，一方面信息已经成为人类的重要资产，在政治、经济、军事、教育、科技、生活等方面发挥着重要作用；另一方面由于信息具有易传播、易扩散、易损毁的特点，信息资产比传统的实物资产更加脆弱和容易受到损害，特别是近年来随着计算机和网络技术的迅猛发展，信息安全问题日益突出，组织在业务运作过程中面临的因信息安全带来的风险也越来越严重。基于大量的信息安全事件案例分析与研究，人们逐渐认识到信息带来的这种风险主要来源于组织管理、信息系统、信息基础设施等方面的固有薄弱环节和漏洞，以及大量存在于组织内、外的各种威胁，因此需要对信息系统加以严格管理和妥善保护，信息安全管理也随之产生。

1.1.1 信息与信息安全

1. 信息

一般意义上，信息可以理解为消息、信号、数据、情报或知识。它可以以多种形式存在，可以是信息设施中存储与处理的数据、程序；可以是打印或书写出来的论文、电子邮件、设计图纸、业务方案；也可以是显示在胶片等载体或表达在会话中的消息。国际公认的 ISO/IEC IT 安全管理指南（GMITS）对信息（Information）给出如下解释：信息是通过施加于数据上的某些约定而赋予这些数据的特定含义。

信息本身是无形的，借助于信息媒体以多种形式存在或传播，它可以存储在计算机、磁带、纸张等介质中，也可以存储在人的大脑里，还可以通过网络、打印机、传真机等方式进行传播。对现代企业来说，信息是一种资产，不仅包括与计算机、网络相关的数据、资料，还包括专利、标准、专有技术、商业档案、文件、图样、统计数据、配方、报价、规章制度、财务数据、工艺、计划、资源配置、管理体系、关键人员等。就如其他重要的商业资产那样，

信息资产具有重要的价值，因而需要进行妥善保护。

所有的组织都有他们各自处理信息的形式。例如，银行、保险和信用卡公司需要处理金融信息，企业、商家需要处理消费者信息，政府管理部门需要处理、存储公众和机密信息等。无论这些信息采用什么样的处理、存储和共享方式，都需要对信息加以安全、妥善的保护，不仅要保证信息处理和传输过程是可靠的、有效的，而且要求重要的敏感信息是机密的、完整的和真实的。为达到这样的目标，必须采取一系列适当的信息安全控制措施，使信息避免一系列威胁，保障业务的持续性，最大限度地降低安全威胁的影响，减少业务和系统的损失。

需要注意的是，从安全保护的角度去考察信息资产，并不能只停留在静态的一个点或者一个层面上。信息是有生命周期的，从其创建或诞生，到被使用或操作，到存储，再到被传递，直至其生命周期结束而被销毁或丢弃，各个环节、各个阶段都应该被考虑到，安全保护应该兼顾信息存在的各种状态，不能有所遗漏。

2. 信息安全

信息安全是一个广泛而抽象的概念，不同领域不同方面对其概念的阐述都会有所不同。建立在网络基础之上的现代信息系统，其安全定义较为明确，即保护信息系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。在商业和经济领域，信息安全主要强调的是消减并控制风险，保持业务操作的连续性，并将风险造成的损失和影响降低到最低程度。

信息作为一种资产，是企业或组织进行正常运作和管理不可或缺的资源。从最高层次来讲，信息安全关系到国家的安全；对组织机构来说，信息安全关系到正常运作和持续发展；就个人而言，信息安全是保护个人隐私和财产的必然要求。无论是个人、组织还是国家，保持关键的信息资产的安全性都是非常重要的。信息安全的任务，就是要采取措施（技术手段及有效管理）让这些信息资产免遭威胁，或者将威胁带来的后果降到最低程度，以此维护组织的正常运作。

随着人类文明的发展与进步，信息处理的方法与技术也在不断发展，从最原始的语言交谈，到古代文字、纸张的发明，再到现代通信、计算机与网络技术的普遍应用，信息的存储、交流、传输、处理的技术与方法越来越多，越来越复杂，信息存储的媒体也越来越多。信息量正在呈几何级数增长，信息的传播容量不断增加、传播速度不断加快、信息资产所面临的安全威胁也在不断地增加，因而信息安全技术得到了相应的发展。当然在不同的发展时期，信息安全的侧重点与信息安全的控制方式与手段也不尽相同。

大致说来，信息安全在其发展过程中经历了3个阶段。

早在20世纪初期，通信技术还不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，人们强调的主要是信息的保密性，对安全理论和技术的研究也只侧重于密码学，这一阶段的信息安全可以简单称为通信安全，即COMSEC（Communication Security）。

20世纪60年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，即INFOSEC（Information Security），具有代表性的成果就是美国的可信计算机系统评估标准（Trusted Computer System Evaluation Criteria，TCSEC）和欧洲的信息技术安全评估标准（InformationTechnology Security Evaluation Criteria，ITSEC）。

从 20 世纪 80 年代开始，由于互联网技术的飞速发展，信息无论是对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间。此时，信息安全的焦点已经不仅仅是传统的保密性、完整性和可用性 3 个原则了，由此衍生出了诸如可控性、抗抵赖性、真实性等其他的原则和目标。信息安全也从单一的被动防护向全面而动态的防护、检测、响应、恢复等整体体系建设方向发展，即所谓的信息保障（Information Assurance）。这一点在美国的信息保障技术框架（Information Assurance Technical Framework，IATF）规范中有清楚的表述。

在由英国标准协会（British Standards Institution，BSI）提出的 BS7799 信息安全管理体系中，信息安全的主要目标是信息的机密性（Confidentiality）、完整性（Integrity）和可用性（Availability）（即通常所说的 CIA）的保持。信息安全是指通过采用计算机软硬件技术、网络技术、密钥技术等安全技术和各种组织管理措施，来保护信息在其生命周期内的产生、传输、交换、处理和存储的各个环节中，信息的机密性、完整性和可用性不被破坏。

（1）机密性（Confidentiality）

信息的机密性是指确保只有那些被授予特定权限的人才能够访问到信息。信息的机密性依据信息被允许访问对象的多少而不同，所有人员都可以访问的信息为公开信息，需要限制访问的信息为敏感信息或秘密信息。根据信息的重要程度和保密要求可以将信息分为不同密级，例如军队内部文件一般分为秘密、机密和绝密 3 个等级。已授权用户根据所授予的操作权限可以对保密信息进行操作，有的用户只可以读取信息，有的用户既可以进行读操作又可以进行写操作。

（2）完整性（Integrity）

信息的完整性是指保证信息和处理方法的正确性和一致性。信息完整性一方面是指在使用、传输、存储信息的过程中不发生篡改信息、丢失信息、错误信息等现象；另一方面是指信息处理方法的正确性，执行不正当的操作有可能造成重要文件的丢失，甚至导致整个系统的瘫痪。

（3）可用性（Availability）

信息的可用性是指确保那些已被授权的用户在他们需要的时候，确实可以访问到所需信息。即信息及相关的信息资产在授权人需要的时候，可以立即获得。例如，通信线路中断故障、网络的拥堵会造成信息在一段时间内不可用，影响正常的业务运营，这就是对信息可用性的破坏。

近年来，随着人们对信息安全认识和理解的深入，一些研究文献进一步拓展认为信息安全的属性应包括：机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、不可否认性（Non-Repudiation）、可控性（Controllability），其中不可否认性也可以定义为认证性（Authenticity）。总的来说，凡是涉及保密性、完整性、可用性、可追溯性、真实性和可靠性保护等方面的技术和理论，都是信息安全所要研究的范畴，也是信息安全所要实现的目标。

1.1.2 信息安全管理的引入

目前信息安全已扩展到了信息的可靠性、可用性、可控性、完整性及不可抵赖性等更新、更深层次的领域，这些领域内的相关技术和理论都是信息安全所要研究的领域。国际标准化组织（ISO）对信息安全的定义是：“在技术上和管理上为数据处理系统建立的安全保护，保

护计算机硬件、软件和数据不因偶然和恶意的原因而遭至破坏、更改和泄露”。

但长久以来，仍有不少人会陷入技术决定一切的误区当中，尤其是那些出身信息技术行业的管理者和操作者。最早的时候，人们把信息安全的希望寄托在加密技术上面，认为一经加密，什么安全问题都可以解决。随着网络的发展和普及，一段时期我们又常听到“防火墙决定一切”的论调。及至更多安全问题的涌现，入侵检测系统（Intrusion Detection System，IDS）、公钥基础设施（Public Key Infrastructure，PKI）、虚拟专用网（Virtual Private Networks，VPN）等新的安全技术与应用被接二连三地提出来，更多的人认为信息安全离不开技术的统领。可这样狭隘地以技术为思路构建信息安全能够真正解决安全问题吗？也许可以解决一部分，但却解决不了根本。实际上，对安全技术和产品的选择运用，只是信息安全实践活动中的一部分，只是实现安全需求的手段而已。信息安全更广泛的内容，还包括制定完备的安全策略，通过风险评估来确定安全需求，根据安全需求选择安全技术和产品，并按照既定的安全策略和流程规范来实施、维护和审查安全控制措施。归根到底，信息安全并不仅是一个技术问题，更需要完善的管理做支撑。

随着信息安全理论与技术的发展，信息保障的概念得以提出并得到一致认可，而在信息保障的三大要素（人员、技术和管理）中，管理要素的作用和地位越来越得到重视。在信息保障的概念中，信息安全一般包括实体安全、运行安全、信息安全和管理安全四个方面的内容。

- 实体安全：保护计算机设备、网络设施以及其他通信与存储介质免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施、过程。
- 运行安全：为保障系统功能的安全实现，提供一套安全措施（如风险分析、审计跟踪、备份与恢复、应急措施）来保护信息处理过程的安全。
- 信息安全：防止信息资源的非授权泄露、更改、破坏，或信息被非法系统辨识、控制和否认。即确保信息的机密性、完整性、可用性、不可否认性和可控性。
- 管理安全：通过信息安全相关的法律法令和规章制度以及安全管理手段，确保系统安全生存和运营。

信息安全的建设是一个系统工程，它需要对信息系统的各个环节进行统一地综合考虑、规划和构架，并时时兼顾组织内外不断发生的变化，任何环节上的安全缺陷都会对系统构成威胁。在这里可以引用管理学上的木桶原理加以说明，木桶原理指的是：一个木桶由许多块木板组成，如果组成木桶的这些木板长短不一，那么木桶的最大容量不取决于长的木板，而取决于最短的那块木板。这个原理同样适用于信息安全：一个组织的信息安全水平将由与信息安全有关的所有环节中最薄弱的环节决定。信息从产生到销毁，其生命周期中包括了产生、收集、加工、交换、存储、检索、存档、销毁等多个过程或事件，表现形式和载体会发生各种变化，这些环节中的任何一个都可能影响整体信息安全水平。要实现信息安全目标，必须使构成安全防范体系的这只“木桶”的所有木板都要达到一定的长度。

由于信息安全是一个多层面、多因素、综合和动态的过程，如果凭着一时的需要，想当然地去制定一些控制措施和引入某些技术产品，都难免存在挂一漏万、顾此失彼的问题，使得信息安全这只“木桶”出现若干“短木块”，从而无法提高安全水平。正确的做法是遵循国内外相关信息安全标准与最佳实践过程，考虑信息安全的各个层面的实际需求，在风险分析的基础上引入恰当控制，建立合理的安全管理体系，从而保证信息资产的安全性；另一方面，

这个安全体系还应当随着环境的变化、业务发展和信息技术提高而不断改进，不能一劳永逸，一成不变。因此，信息安全的实现是一个需要完整的技术和管理体系来保证的持续过程。

1.2 信息安全管理的内涵

1.2.1 信息安全管理及其内容

1. 信息安全管理的定义

信息安全管理是通过维护信息的机密性、完整性和可用性等，来管理和保护信息资产的一项体制，是对信息安全保障进行指导、规范和管理的一系列活动和过程。信息安全管理是信息安全保障体系建设的重要组成部分，对于保护信息资产、降低信息系统安全风险、指导信息安全体系建设具有重要作用。

2. 信息安全管理的内容

信息安全管理应当涉及信息安全的各个方面，包括制定信息安全政策、风险评估、控制目标与方式选择、制定规范的操作流程、对人员进行安全意识培训等一系列工作。按照信息安全管理国际标准 ISO/IEC 27002《信息安全管理实用规则》，一般通过以下 11 个领域建立管理控制措施，构建起一张完备的信息安全“保护网”，保证信息资产的安全与业务的持续性。

（1）安全方针和策略

为信息安全提供管理指导和支持。

（2）组织安全

即建立管理架构，启动、管理和维护信息安全，并保护被外部组织访问、处理、沟通或管理的信息及信息处理设施的安全。

（3）资产分类与控制

通过对信息资产进行分类、标识、责任划分以及风险评估与控制，确保信息资产受到与其安全要求相对应的保护。

（4）人员安全

通过安全职责、用户培训及安全事故报告等方面，确保将人为因素对信息资产的安全威胁降到最低。

（5）物理与环境安全

通过对安全区域、设备及信息媒体的安全控制，保证信息的安全。

（6）通信、运行与操作安全

通过明确作业程序及责任、第三方服务交付管理、系统规划与验收、防范恶意与移动代码、备份与恢复、网络安全管理、存储媒体控制、信息与软件交换控制、电子商务安全控制及安全监视等，保证信息系统在通信、运行和操作过程中的安全。

（7）访问控制

包括明确访问控制要求、用户访问管理、明确用户责任、网络访问控制、操作系统访问控制、应用程序访问控制及移动计算和远程工作控制等。

（8）系统获取、开发与维护

通过明确系统安全需求、应用系统安全控制、密码控制、文档安全控制、开发与支持过

试读结束：需要全本请在线购买： www.ertongbook.com