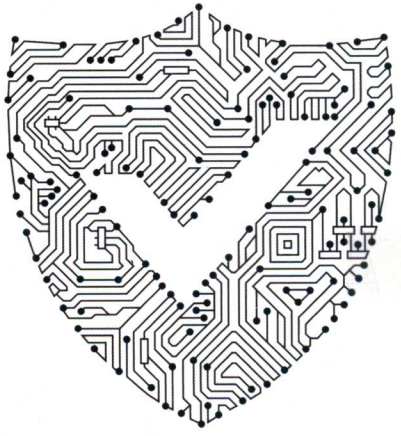
海军新军事变革丛书

总策划：魏　刚　　主　编：马伟明

# 信息系统安全基础

（原书第2版）



[美] David Kim
Michael G. Solomon　著

朱婷婷　陈泽茂　赵　林　译
杨　波　主审

FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY, 2E

中国工信出版集团

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

海军新军事变革丛书

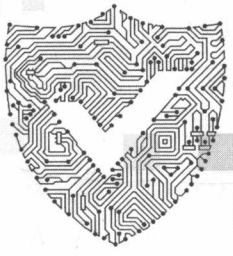
总策划：魏　刚　　主　编：马伟明

# 信息系统安全基础

FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY, 2E

[美] David Kim
Michael G. Solomon　著

朱婷婷　陈泽茂　赵　林　译
杨　波　主审



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

版权贸易合同登记号 图字：01-2016-0783

**图书在版编目（CIP）数据**

信息系统安全基础 /（美）戴维·吉姆（David Kim），（美）迈克尔·G. 所罗门（Michael G. Solomon）著；朱婷婷，陈泽茂，赵林译. —北京：电子工业出版社，2020.4
（海军新军事变革丛书）
书名原文：Fundamentals of Information Systems Security, 2e
ISBN 978-7-121-37899-7

Ⅰ. ①信… Ⅱ. ①戴… ②迈… ③朱… ④陈… ⑤赵… Ⅲ. ①信息系统－安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2019）第 258091 号

责任编辑：王小聪
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：720×1000　1/16　印张：30.5　字数：564 千字
版　　次：2020 年 4 月第 1 版（原书第 2 版）
印　　次：2020 年 4 月第 1 次印刷
定　　价：135.00 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）88254888，88258888。

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。

本书咨询联系方式：（010）57565890，meidipub@phei.com.cn。

# 海军新军事变革丛书

# 信息系统安全基础

**主译** 朱婷婷 陈泽茂 赵 林
**翻译** 付 钰 付 伟 严 博 秦艳琳 吴邱涵
**主审** 杨 波

# 《海军新军事变革丛书》第三批总序

当今世界，新一轮科技革命和产业变革正在加速推进，以信息技术为引领，人工智能、生物科学、大数据、新材料、新能源等技术发展运用、交叉融合和相互渗透，正逐步改变着人类社会形态和生产生活方式。高新技术的发展和世界安全态势的演变，同样催生当今世界军事领域的深刻变革，在广度、深度上已超越以往历史上任何一轮军事变革。这次变革以安全态势演变为动因、以高新技术特别是信息技术发展为动力、以军事观念转变为牵引、以军事体系调整为中心，覆盖军事领域各个方位和全部系统，涉及军事理论、军事战略、战争形态、作战思想、指挥体制、部队结构、国防工业等方方面面，形成信息主导、体系支撑、精兵作战、联合制胜的新态势，数字化、网络化、智能化和系统化将贯穿决策指挥、组织形态和战场战法全过程，渗透到各个方面，作战域将加速向网络、电磁、深海、太空、极地等战略新疆域拓展，其所产生的影响，必将影响未来世界格局，决定各国军事力量对比。

习主席曾深刻指出："每一次科技和产业革命都深刻改变了世界发展面貌和格局。一些国家抓住了机遇，经济社会发展驶入快车道，经济实力、科技实力、军事实力迅速增强，甚至一跃成为世界强国。"党的十八大以来，党中央、中央军委着眼于实现中国梦、强军梦，制定新形势下军事战略方针，全力推进国防和军队现代化，军队改革取得历史性突破，练兵备战有效遂行使命任务，现代化武器装备加快列装形成战斗力，军事斗争准备稳步推进，强军兴军不断开创新局面。党的十九大，吹响了"到 21 世纪中叶把人民军队全面建设成世界一流军队"的时代号角，郑重宣告国防和军队建设全面迈进新时代。经略海洋、维护海权、建设海军始终是强国强军的战略重点，履行新时代军队历史使命，海军处在最前沿、考验最直接，职能最多样、任务最多元，需求最强劲、发展最迫切。瞄准世界一流、建设强大的现代化海军，我们更须顺应新形势，把准新趋势，进一步更新观念、开阔视野，全面深入实施科技兴军战略，瞄准世界军事科技前沿，坚持自主创新的战略基点，加强前瞻性谋划、体系化设计，加快全域全时全维的信息化、

智能化建设，抢占军事科技战略性、前沿性、颠覆性发展制高点，努力实现从跟跑、并跑到领跑的历史性跨越。

根据海军现代化建设的实际需求，2004 年 9 月，海军装备部与海军工程大学联合组织一批学术造诣深、研究水平高的专家学者，启动了《海军新军事变革丛书》的编撰工作。2004 年至 2009 年，第一批丛书陆续出版，集中介绍了信息技术及其应用成果。2009 年至 2017 年，第二批丛书付梓，主要关注作战综合运用和新一代武器装备情况。该丛书具有鲜明的时代特征和海军特色，对推进中国特色军事变革要求，谋划海军现代化建设具有很好的参考价值，在部队、军队院校、科研院所、工业部门均被广泛使用，深受读者好评。丛书前两批以翻译出版外文图书和资料为主，以自编海军军内教材与专著为辅，旨在借鉴外国海军先进技术和理念，反映世界海军新军事变革中的新观念、新技术、新理论，着重介绍和阐释世界新军事变革的“新”和“变”。为全面贯彻落实习主席科技兴军的战略思想，结合当前世界海军发展趋势和人民海军建设需要，丛书编委会紧跟科技发展步伐，拟规划出版第三批丛书。在前期成果的基础上，第三批丛书计划逐步从编译转向编著，将邀请各领域专家学者集中撰写与海军人才培养需求密切相关的军事理论和装备技术著作，这是对前期跟踪研究世界海军新军事变革成果的消化、深化和转化。

丛书的编撰出版凝结了编委会和编写人员的大量心血和精力，借此机会，谨向付出辛勤劳动的全体人员致以诚挚的敬意，相信第三批丛书定会继续深入贯彻习主席强军思想，紧盯科技前沿，积极适应战争模式质变飞跃，研判战争之变、探寻制胜之法，为建设强大的现代化海军带来新的启迪、新的观念、新的思路，不断增强我们打赢信息化战争、应对智能化挑战的作战能力。

海军司令员 沈金龙

2018 年 6 月 2 日

# 译者序

信息技术（Information Technology，IT）的发展，带来了劳动生产的自动化、工作的多样化、生活的便捷化、社会交往的多元化，也促进了全球资源的优化配置以及各个领域发展模式的创新。信息化快速渗透至国民生活的各个领域，进一步对政治、经济、文化产生非常深刻的影响。其中，网络通信技术的飞速发展使“万物互联”成为可能，它大大改变了人们的沟通、生活、工作模式，国家关键基础设施基于网络实现了高度互联，世界各国军事力量、经济力量、社会生活、国家管理广泛依赖于以网络为基础的信息系统。与信息技术发展结伴而生的是信息安全问题的凸显，围绕信息获取、使用和控制的国际竞争日趋激烈，关键基础设施及其网络系统成为了攻击目标，这些严重威胁着国家安全与社会稳定。（确保信息及信息基础设施的安全具有重要的作用和意义。信息安全从业人员的能力素质是影响高效安全保障的实现重要要素）。基于此在“帮助教育信息系统安全实践者”的驱动下，作者编著了此书。该书是一本源于信息安全实践而又指导信息安全实践的著作，原作著者 David Kim 是资深的信息安全专家，拥有自己的信息安全服务公司，在 IT 安全行业从业 28 年之久。他还是一名兼职教授，在全美各地教授学生网络安全知识。书中拥有大量的 IT 安全技术、管理、教育方面的详实资料和原创性的观点，这些与原著者丰富的工作经验和阅历有着紧密的关系。

下面从译者的角度，对书中的内容进行概括性的评述，给出如下“导读”，使读者能够在了解著者写作目的的基础上，初步了解该领域，明确本书能够提供哪些知识、满足怎样的阅读需求，从而快速确定该书是否适合阅读、准确定位内容，满足有限时间内准确选读的需要。

## 一、关于作者

原著作者 David Kim 是 Security Evolution（SEI）公司总裁，该公司位于费城城郊，为全球公共和私营部门客户提供安全管理、风险评估和法律咨询等服务，

客户主要来源于医疗、银行、政府和机场等机构，它的IT安全咨询服务包括安全风险评估、脆弱性评估、合法性审计以及为企业设计多层次安全解决方案等。此外，该公司还提供系统可用性相关的服务，该服务包含开发制定业务持续性和灾难恢复计划等。David Kim先生在IT及IT安全的工程技术、管理技术、销售和市场管理等方面拥有30多年的工作经验。在局域网/广域网、互联网、企业内部网络管理以及音/视频信息技术安全、数据中心网络架构等方向，经验丰富。他是一位很有成就的作家和兼职教授，在全美很多地方教授学生网络安全方面的知识。

Micheal G. Solomon是一位全职的安全演说家、顾问，也是一名作家。曾任大学讲师，主要研究方向为安全开发和评估。自1981年起长期担任IT行业的顾问，并为100多家公司和机构提供项目服务。1998—2001年，他在肯尼索州立大学计算机与信息科学系任教，讲授软件项目管理、C++编程、计算机组成与体系结构、数据通信等课程。他于1987年毕业于肯尼索州立大学，获得计算机科学理学学士学位；于1998年在该大学获得数学和计算机科学理学硕士学位；目前正在埃默里大学攻读计算机科学和信息学博士学位，主要研究方向为不可信云环境下的安全保障。他还撰写和参与编写了诸多安全类书籍，包括Security Strategies in Windows Platform and Applications（Jones & Bartlett Learning，2011），Computer Forensics JumpStart（2nd）（Sybex，2011），Solomom coauthored Information Security Illuminated（Jones & Bartlett，2005），Security +Lab Guide（Sybex 2005），PMP ExamCram2（Que，2005）等书籍，同时还编写了Learnkey CISSP Prep 和PMP Prep网络课程教学的教材，并进行网络授课。

## 二、内容简介与评述

本书是Jones & Bartlett Learning（www.jblearning.com）出版的信息系统安全与保障系列丛书（Information Systems Security & Assurance Series，ISSA）中非常重要且基础性的一本书。书中包含信息安全需求、信息安全技术以及信息安全相关的标准、教育、法律、认证等内容。通过本书的阅读，读者能够了解到信息系统安全主要驱动因素、保障信息系统安全的核心技术、信息安全领域标准化组织和相关标准、信息系统安全知识学习和技能培训途径、广泛被认可的信息安全认证以及美国相关信息安全法律等。

本书的编著以指导信息系统安全实践者的学习和实践为目标。原著者在信息领域有着丰富的从业经验，多年实践工作经验支撑其总结、提炼出了信息化技术发展如何催生了信息安全需求、以及如何驱动了信息安全业务的发展等内容。作为信息安全领域资深的专家，他熟知信息安全从业人员需要掌握的知识和应具备的技能，以信息安全行业内权威的（ISC）²（以顶尖教育计划享誉全球，其认证在全球被誉为信息安全认证的“金牌标准”）SSCP®认证所需掌握的知识为依据，结合自己实践经验，构建了本书信息安全技术部分的知识体系，并总结提炼了本书的内容。除此之外，他还清晰的认识到了解、理解行业标准和相关法律对更好地开展信息安全工作非常重要，结合信息安全行业特点以及工作经验，对信息安全领域影响力较大的标准化组织、标准以及相关垂直行业在美国应该遵循的法律进行了梳理分析。为了更好地帮助、指导各类信息安全实践者快速、准确找到适合的学习途径和方法，他还对目前常见的几类信息系统安全教育与培训方式的特点及课程获取途径进行了总结，结合从业经验对行业内权威的信息安全认证进行了分析。

以下对本书内容进行概括和评述。

**1. 关于信息安全需求**

信息安全问题伴随着 IT 应用而突显，为了避免读者概念混淆造成对书中内容理解不清，这里对易混淆的信息安全相关概念进行阐述。

**信息安全（Information Security）**

信息安全的需求和内涵不断拓展，通信安全、计算机安全、网络安全、信息系统安全、网络空间安全等概念逐步被提出。信息安全最初主要指保护信息系统中处理、存储、传输秘密信息的安全，注重信息的机密性，主要强调通信安全（Communication Security，COMSEC）（例如，美国海军早期 COMSEC 的研究课题着重研究信息的机密性保护问题）。随着个人计算机及信息系统广泛应用、分布式计算的发展，数据、系统访问控制的重要性日益突出，安全概念扩展至完整性保护。此时，更加强调计算机安全（Computer Security，COMPSEC）。网络的发展促使信息系统的应用范围不断扩大，使网络成为计算机系统正常运行、发挥效能的重要支撑。这个时期，人们更加重视网络虚拟性带来的逻辑安全问题，网络安全（Network Security，NETSEC）的防护需求突出。随着信息基础设施的广

泛构建，其保护要求越来越突出，信息安全内涵由通信安全、计算机安全、网络安全等运行安全（Operation Security，OPSEC）扩展至物理安全（Physical Security，PHYSEC）。信息系统应用越来越广泛，信息系统的效能发挥与网络、信息系统基础设施密不可分。此时，信息系统可用性成为关注的重点，信息安全更强调信息安全保障的整体性。“通信安全”“计算机安全”“网络安全”已成为信息安全的子域，信息安全包含更加宽泛的概念，ISO/IEC 17799：2005 中指出“信息安全通过实施一组合适的控制达到，包括策略、措施、过程、规程、组织结构及软件和硬件功能”。随着计算机和网络技术的加速发展，信息安全的技术要求集中表现在 ISO 7498-2 标准陈述的各种安全机制中，这些安全机制的共同特点就是对信息系统的机密性、完整性和可用性进行静态保护。随着信息安全技术的发展，信息安全的方法拓展到了信息保障范畴，信息安全技术已经不再是以单一的防护为主，而是包括了防护、检测、响应和恢复几个关键环节的动态体系。

**信息系统安全（Information System Security）**

在信息系统研究领域内，信息系统安全是广泛使用的概念。信息系统是由计算机软件及硬件、网络和通信设备、信息资源、信息用户以及规章制度组成的以处理信息流为目的的人机一体化系统，其基本功能包括信息输入、存储、处理、输出和控制。本书从实际应用的角度出发，提出了信息系统安全的定义：“信息系统由硬件、操作系统、安装在设备中的各种应用软件以及存储的数据组成，信息系统安全是保障信息系统及其中存储数据的相关活动的安全。”

**网络空间安全（Cyberspace Security）**

网络空间（部分文献将其直译为赛博空间）的概念随着人们对网络战的研究加深不断演进。美国空军发布的《美国空军网络空间战略司令部战略构想》中将网络空间定义为：“通过网络系统和相关物理基础设施，使用电子和电磁频谱来存储、修改或交换数据的物理域，主要由电磁频谱、电子系统及网络化基础设施三部分组成。”网络空间的互联互通旨在交换、传输、存储和处理各类信息数据，是各类信息系统的集合。

ISO/IEC 27032：2012 中指出“网络空间安全不仅包含对信息资源的保护，还包括了对其他资产的保护，例如，对人类自身的保护”。网络空间安全在各种部署模式中具有特定的安全需求，例如，移动互联网安全、电信网安全、可信计

算安全、云计算安全、大数据安全、物联网安全、广电网安全等。同时，也囊括了不同应用场景衍生的特定安全保障，例如，在线社交网络、安全工业控制系统安全、支付安全以及针对全球广泛应用的信息系统而存在的互联网安全治理等。从网络空间载体、资源、主体和操作等方面分析，网络空间安全，包括网络空间中的电磁设备、信息通信系统、运行数据、系统应用中存在的安全问题。既要保护包括互联网、电信网与通信系统、传统系统与广电网、计算机系统、关键工业设施中的嵌入式处理器和控制器等在内的信息通信技术系统及其所承载的数据免受攻击，也要防止和应对运用或滥用信息系统而影响政治安全、经济安全、文化安全、社会安全、国防安全等。

从信息安全内涵的演变可以看出，信息技术驱动了信息安全需求的不断丰富，推动了学术界、产业界对信息安全理解和认识的加强。但目前为止，严格地说，没有明确的定义，仅有一些来源于不同理解角度的相关描述。从描述中可知，信息安全、信息系统安全、网络空间安全的内涵有交叉也有不同。信息系统安全是信息安全与网络空间安全的重要分支，传统的信息安全侧重于突出保障信息及其相关资源的机密性、完整性及可用性，而网络空间安全更侧重于网络空间范畴内的信息资源以及其他资源的安全保护。

本书第一部分作者着重解答了为什么需要保障信息安全这个问题，围绕实际应用中典型 IT 架构分析了安全需求产生的内化因素与外在因素，包括自身架构及通信模式中存在的安全风险、威胁和脆弱性，恶意代码带来的威胁以及业务驱动的安全需求。随着“大智移云”时代（即以大数据、智能化/物联网、移动互联网、云计算共同驱动的时代）的到来，信息产业驱动力正从产品转向服务，并呈现横向扩展、多点驱动的趋势。作者对信息安全需求的分析仍然适用于当今信息产业新环境。

### 2. 关于信息安全技术

信息安全从业人员通常会承担安全技术实践和系统运维的工作。这样的工作要求其具备依照信息安全策略、流程和要求，实施、监控与管理 IT 基础设施，从而确保数据、系统机密性、完整性与可用性的能力。本书围绕这样的能力需求，参考(ISC)$^{2}$ ®SSCP®认证技术体系，构建了信息安全技术部分的内容体系。该部分内容涵盖了七大知识领域，即：访问控制、安全运营与管理、风险识别、监控与

分析、事件响应与恢复、密码学、网络与通信安全、系统与应用安全；内容覆盖了信息系统安全防护、检测、响应以及恢复各个关键环节。这些内容包含了信息安全从业人员当前面临的与工作实践最为相关的问题以及解决问题的最佳实践方式，准确地描述了一线信息安全从业人员应掌握的安全知识和具备的技能。

**访问控制**

访问控制是实现信息系统安全保障的基础和核心。本书第 5 章着重阐述了如何实现访问控制。书中，访问控制部分的内容涵盖了身份认证、访问控制与安全审计三个重要机制。身份认证是信息系统安全的第一道防线，其目的是阻止非法用户进入系统。标识、验证是身份认证的两个重要环节：标识是身份认证的基础，它是指为每个用户取一个系统可以识别的内部名称，即用户标识符，其目的是便于控制和追踪用户在系统中的行为。用户标识必须唯一、不能被伪造，且应防止用户冒充。验证是用户标识符与用户联系的过程，是证实某人或某物是否名副其实或是否有效的过程，该过程又被称为认证。这里对某人的鉴别是指对主体的鉴别；对某物的鉴别是对客体有效性的鉴别。授权是访问控制技术的中心环节，它是在通过身份认证阻止非法用户进入系统的基础上实现的对合法用户权限的授予，通过限制不同用户系统访问权限实现系统的安全保护，它是信息系统安全保障最重要的环节。追溯包含记录、查证两部分内容，即记录用户在系统中的行为，提供追查违反安全策略行为的依据。追溯是实现安全审计的前提，其目的是为守住信息系统安全的最后一道防线提供依据。

在实际应用中，标识、验证、授权、追溯，通常是广义上实践访问控制的重要环节，四个环节之间有着紧密的联系，如果没有合理的用户标识，验证、授权、追溯就无法正确实现：标识是它们实现的基础；授权是以正确验证为前提，只有通过验证的合法用户才能进行系统访问授权；追溯是对标识、验证、授权与访问等行为的记录，为事件重现提供依据。因此，作者从指导实践的角度出发，以标识、验证、授权、追溯的实现为主线组织第 5 章内容。

在国内外的部分教材中将身份认证、访问控制、安全审计作为独立的章节进行介绍，读者亦可以从其他教材的身份认证、访问控制、审计等章节中获取本章相关的内容。

**安全运营与管理**

信息安全技术与产品的使用者需要系统、科学的安全管理知识和手段帮助他们使用好安全技术与产品，从而有效解决面临的信息安全问题。当前，安全管理技术已经成为信息安全技术的一部分，它属于安全支撑技术的范畴，涉及安全管理制度的制定、物理安全管理、系统与网络安全管理、信息安全等级保护及信息资产的风险管理等内容，它是实现信息系统安全的重要环节之一。本书第 6 章、第 7 章、第 8 章均涉及信息安全管理的相关内容。

本书第 6 章涵盖了(ISC)²®SSCP®认证技术体系第二大知识领域安全运营与管理的内容。该部分包含安全管理与安全系统开发两部分内容，着重为读者根据信息安全策略、流程和要求实施信息安全保障提供指导。信息安全专业人员需要理解安全操作以及管理中基础、固定的安全流程、在安全管理工作中如何实现安全计划（包括设计、实施以及监控组织的安全计划等）；需要了解执行安全计划时必须符合的安全流程，遵守的相关职业道德标准；掌握实现安全流程的方法手段以及如何将现有各项方针、政策、标准应用到工作计划中构建安全框架；了解数据分类标准，理解数据分类如何影响决策过程；掌握如何对系统变更进行配置管理，理解配置控制、变化控制如何影响管理过程。本书第 6 章内容能够满足读者如上学习需求。

除此之外，作者在多年的工作实践中认识到掌握系统生命周期（SLC）和系统开发生命周期（SDLC）、理解为什么在软件开发过程中需要考虑安全问题以及需要考虑哪些安全问题，对于更好地实现安全运营与管理至关重要。因此，在第 6 章中系统介绍了软件开发中最常用的系统生命周期与系统开发生命周期方法以及软件开发的模型，分析了方法每个步骤中需要考虑的安全因素。

**风险识别、监控与分析**

在实际应用中，通常会采用诸多安全控制措施保护信息资产。既然采取了保护措施，就应该确保每个措施对安全威胁的有效性。不针对任何威胁的安全控制措施会带来不必要的开销且对安全起不到任何作用。因此，掌握系统运行状态，准确把控系统以及安全控制措施是否按照预期运行，从而分析和识别安全风险，对于保障信息系统安全至关重要。审计、监控、测试是了解系统运行状态、发现系统安全风险的重要途径。本书第 7 章审计/测试和监控对此部分内容进行了描述。

审计、监控、测试从事后检查、实时监察、主动探查三个方面实现了解系统安全状态和安全风险的目标。审计通常是一种事后检查的方式，它以第5章审计记录技术为支撑，开展安全性审计。这里需要强调：安全性审计区别于传统的系统审计，它的实施依赖于用户的定义，通常仅审核系统安全机制部署、安全策略实施、安全状态相关的系统行为。监控是实时了解系统安全状态的主要手段，部分功能的实现以审计记录为基础，着重监测对系统产生安全威胁的异常行为。安全监测是一种技术或一种手段。测试是一种主动探查的手段，安全测试的主要目的是识别系统中未被纠正的脆弱性。一个系统可能在某个时段安全，但用于新的服务或新的应用时就可能存在脆弱性。因此，测试的目的就是要发现新的脆弱性，从而应对它们。

本书着重介绍了安全审计、系统监控、系统安全性测试的有关知识。读者可以了解到审计如何助力于保障系统安全，学习到为什么需要审计、如何制定审计计划、审计基准是什么、如何搜集所需要的信息来进行高质量的审计、如何进行日志管理、如何实现系统监控及安全性测试等，从而掌握把控系统安全风险及状态的方法。

**事件响应与恢复**

当检测到系统存在安全风险或系统遭受到损坏后，应该采取相应的措施降低安全风险的危害，帮助系统迅速恢复。此部分内容在书中第8章风险、响应与恢复中进行了描述，是信息安全保障技术框架中响应与恢复部分的内容。

信息安全专业人员实践中通常需要从以下几方面开展工作：识别组织承受的风险；通过实施控制，尽可能地阻止破坏；准备好应对无法阻止事故的计划和流程。这些内容都属于风险管理的范畴。通过本书第8章内容的阅读，读者能够了解风险管理的原因、处理方法过程，明白业务连续性计划（BCP）如何帮助组织确保灾难不会导致组织业务中断，掌握风险分析、响应以及评估的措施和方法，掌握备份的方法以及可以用来进行灾难恢复的备份模型、事故响应步骤，理解事故响应在风险、响应与恢复进程中的重要性，掌握灾难恢复的主要步骤，明确信息安全专业人员在整个灾难恢复计划中扮演的角色。

**密码学**

数据通信的机密性需求，推动了人们对密码学理论、技术的研究，并使其应

用逐渐成熟。密码技术是信息安全的基础技术，密码系统的安全性赖于密钥的安全性，而不是密码算法的机密性。

密码技术主要包括密码算法、密码协议的设计与分析。密码算法包括分组密码、序列密码、公钥密码、杂凑函数、数字签名等，它们在不同的场合分别用于提供机密性、完整性、真实性和不可否认性保护，是构建安全信息系统的基本要素。密码协议是在消息处理环节采用了密码算法的协议，它们运行在计算机系统、网络或分布式系统中，为安全需求方提供安全的交互操作。密码分析技术是指在获得一些技术或资源的条件下破解密码算法或密码协议的技术。

本书第 9 章密码系统介绍了密码学的基本原理及其商业应用。读者可以通过本书了解到：密码学基本概念及各种商业事务的安全需求、如何将密码技术应用于这些安全需求、如何区分基于密码学设计的各类安全产品以及对称密钥密码体制、非对称密钥密码体制的优缺点等。

**网络与通信安全**

对于今天的大多数组织机构来说，网络和通信是业务基础设施的关键组成部分，它的不可用或者出错会影响组织机构的正常运行。网络与通信安全的目标是满足组织对网络机动性、完整性、可用性的基本需求。信息安全实践者需要掌握网络与通信的基础知识、以及网络安全技术。

本书第 10 章网络与通信安全介绍了网络开放系统互联参考模型（Open Systems Interconnection Reference Model，OSI）、网络拓扑、传输控制协议/因特网互联协议（TCP/IP）、无线网络以及网络安全的相关知识。读者能够了解到 OSI 参考模型以及在建设和使用网络及其资源时 OSI 参考模型所起的参考作用、TCP/IP 协议体系以及网络层协议、网络安全防护基本工具、无线网络工作原理及其可能对企业安全带来的威胁。通过学习及实践，读者能够更好地理解为什么需要安全策略、标准和技术以及 IT 基础设施安全为什么取决于其最薄弱的环节。

**恶意代码检测与防范**

恶意代码是指能够在计算机系统中进行非授权操作，给系统安全性带来潜在威胁的代码。（根据编码特征、传播途径、攻击形式及在目标系统中的生存方式等因素恶意代码通常被划分为计算机病毒、网络蠕虫和特洛伊木马等类型。它以破坏系统、盗取重要数据为目标，是互联网连接设备或计算机的主要威胁。）通

常针对信息安全的三个属性进行攻击：机密性攻击，即泄露隐私信息；完整性攻击，即篡改系统或数据信息；可用性攻击，即破坏数据、软件、硬件的应用。近年来，全球频现重大安全事件，2017 年爆发的新型“蠕虫式”勒索软件 Wanna Cry、2018 年 Facebook 数据泄露事件、2019 年德国政客私人信息泄露事件等均反映了恶意代码的严重影响。

恶意代码检测与防范被广大计算机用户熟知，但技术实现比较复杂。在原理上，防范技术需要利用恶意代码的特征来检测并阻止其运行，但对于不同恶意代码，其特征可能差别很大。目前，已有很多能够帮助发掘恶意代码的静态和动态特征的技术，也出现了一系列在检测恶意代码、阻断其恶意行为的技术。

本书第 11 章恶意代码及防范着重介绍了恶意代码的特点、结构、类型、发展历史、商业威胁；从防御实践的角度出发，阐述了防范工具与技术及检测工具及技术。读者可以了解不同类型的恶意软件及其操作、垃圾邮件和间谍软件及其影响、不同类型的网络攻击以及保护网络免受攻击的方法、计算机病毒的历史及威胁、实现不同类型攻击以及攻击防范的方法、事件检测技术与方法等。

### 3. 关于信息安全标准、教育、认证及法规

信息安全从业人员除了掌握信息安全技术之外，还需要了解信息安全标准、法规以及支撑从业者学习、深造所需的教育与认证相关知识。

#### 信息安全标准

在实施信息系统安全防护时，很难从同一厂家获得所有信息安全产品，需要从不同的供应商处购买相关产品，并使这些软件、硬件协同工作。统一的标准是创建和维护市场竞争的必要条件，也是可确保不同国家的产品相互兼容、在计算环境中协同工作的重要依据。因此，从业人员需要掌握这些通用标准和技术规范，以此指导使用遵循相同标准、来源不同的产品并使其协同工作。研究学习好这些标准对从事信息安全工作非常重要。

随着信息技术的不断发展，信息安全标准也随之逐步更新与发展。在书中作者依据多年的从业经验，对信息安全领域著名的标准化组织及应用广泛的标准进行解读，这些标准均为计算机、网络产品与服务的通用标准。读者可以以此为依据开展信息系统安全保障相关工作。