注册信息安全专业人员资质认证教材

HZ BOOKS
华章科技

Information Assurance

信息安全保障

吴世忠 江常青 孙成昊 李华 李静 编著

机械工业出版社
China Machine Press

Information Assurance

信息安全保障

吴世忠 江常青 孙成昊 李华 李静 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

信息安全保障 / 吴世忠等编著 . —北京：机械工业出版社，2014.10

ISBN 978-7-111-48250-5

I. 信… II. 吴… III. 信息安全 IV. TP309

中国版本图书馆 CIP 数据核字（2014）第 236714 号

本书从我国国情出发，结合我国网络基础设施和重要信息系统安全保障的实际需求，以知识体系的全面性和实用性为原则，明确了信息安全专业人员应该掌握的信息安全技术方面的主体内容和相关的法律法规。

本书涵盖信息安全保障、技术、工程、管理、法律、法规及标准等领域知识，内容全面、实用。第 1 ~ 2 章，介绍了信息安全保障的基础知识和相关实践，讲述了信息安全保障模型、现状、主要工作内容和工作实践。第 3 ~ 6 章，讲述信息安全管理的方方面面，涵盖信息安全管理、信息安全风险管理、信息安全体系建设、灾难发生时的应急响应和灾难恢复。第 7 章讲述信息内容安全，主要为信息内容安全基础、我国网络舆情概况、网络舆情管理等。第 8 ~ 9 章为信息安全工程方面，讲解了信息安全工程基础、实施、监理，以及信息工程能力评估的方法、领域及作用等。第 10 ~ 12 章讲述信息安全相关的法规、政策、标准和道德规范。

信息安全保障

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）

责任编辑：高婧雅　　责任校对：殷　虹

印　　刷：中国电影出版社印刷厂　　版　　次：2014 年 11 月第 1 版第 1 次印刷

开　　本：185mm × 260mm　1/16　　印　　张：17.25

书　　号：ISBN 978-7-111-48250-5　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991　88361066　　投稿热线：（010）88379604

购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

前　言

随着信息化不断深入，信息安全上升到关系社会稳定、经济发展和公民权益的地位，成为国家安全的重要组成部分。在整个信息安全保障工作中，人是最核心、最活跃的因素，信息安全保障工作最终也是通过人来落实的。因此，加快信息安全人才培养体系建设是发展我国信息安全保障体系必备的基础和先决条件。

多年来，国家高度重视我国信息安全人才队伍的培养和建设，明确提出要加强信息安全人才培养。2003 年 9 月，中共中央办公厅、国务院办公厅转发了《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发 [2003] 27 号），提出了“加快信息安全人才培养，增强全民信息安全意识”的指导精神。中国信息安全测评中心依据中央赋予的职能，自 2002 年起，积极推动我国信息安全专业人才培养工作。一方面支持并配合国内多所大学开办了信息安全专业，有力促进了信息安全学历教育的开展；另一方面在原国务院信息化办公室的支持下，开创性地开展了信息安全职业教育与能力认证工作，面向社会提供“注册信息安全专业人员”（CISP）培训服务，十余年来培养专业人才逾万名，为党政军机关和职能部门以及金融、交通、能源等行业和国有大型企业的信息安全保障工作填补了专业人才队伍的空白。

教材和知识体系是信息安全职业培训认证工作的核心要素。中国信息安全测评中心在全面考察国际知名信息安全职业教育知识体系的基础上，汇集国内诸多院士、专家和学者智慧，汲取教学实践体验，提出信息安全人才需要全面涵盖理论、技术、管理、工程、标准和法律法规等知识域，在此基础上编撰了《信息安全理论与技术》、《信息安全工程与管理》及《信息安全标准与法律法规》系列教材，于 2003 年由人民邮电出版社正式出版。该系列教材填补了国内空白，成为信息安全保障工作中的必备参考书。

信息安全是动态发展变化的。新技术不断推陈出新，信息安全态势不断演变，需要不断地更新知识。经过十余年的积累，我们编撰了《信息安全技术》和《信息安全保障》两本书，这是在原版本系列教材基础上的全面修订，经过了三年试用和多次完善。与上版相比，修订后的教材具有以下三个特点。

一是主线更清晰，内容更全面。《信息安全技术》增加了安全攻击与防护、软件安全开发等章节。《信息安全保障》新增了信息安全管理基础、信息安全风险管理、信息安全等级

保护等章节，进一步充实了信息安全法律、法规和标准体系等方面的内容。整套教材系统地阐述了当前我国信息安全保障体系的主要工作，以及各项工作涵盖的关键技术。

二是知识进行了全面更新。在《信息安全技术》中，增加了云计算、物联网和工业控制系统等新领域的安全防护技术，以及主流安全管理平台、统一威胁管理系统、网络准入控制系统、Web 应用安全防护产品的技术原理与应用。在《信息安全保障》中，信息安全战略、法律、法规、政策及标准更新截至 2013 年。本套教材全面体现了信息安全领域各方面的最新发展状况，与国外同类信息安全培训教材知识体系总体保持同步。

三是吸收了十余年来中国信息安全测评中心在漏洞分析与风险评估等领域的最新科研成果与工作积累，同时，汇聚了知名高校、科研院所、行业及产业信息安全专家的知识与经验。与国外同类信息安全培训教材相比，本套教材更加贴合我国信息安全保障的实际工作要求，技术理论、政策指导与实践应用相结合，满足国家对信息安全人才的深层次需求。

本套教材以知识体系的全面性和实用性为原则，涵盖信息安全保障、技术、工程、管理、法律、法规及标准等领域知识，为信息安全管理与技术人员解决实际工作问题提供参考。本套教材主要面向国家部委、重要行业、科研院所及企事业单位的信息安全从业人员，适用于信息技术产品研发测试、信息系统安全规划与建设运维、信息安全服务等方面的专业技术人员，以及信息安全总体规划、策略制度制定、风险评估和监督审计等方面的管理人员。

本套教材在修订完善的过程中得到社会各界人士的关心与支持，特别是中国信息安全测评中心刘晖、郭涛、彭勇、张涛、班晓芳、姚轶崭、郭颖、戴忠华、任望、王庆、王星、邹静，上海信息安全工程技术研究中心谢安明，清华大学叶晓俊，北京交通大学李勇，中国科学院软件研究所苏璞睿，华东师范大学张雪芹，北京信息科技大学刘凯，北京江南天安科技有限公司陈冠直、胡杰，北京时代新威信息技术有限公司王连强，上海三零卫士信息安全有限公司邬敏华、陈锡军、陈长松，北京奇虎测腾科技有限公司张奕，南京翰海源信息技术有限公司方兴，在此表示衷心的感谢。

教材中不妥或错误之处恳请广大读者批评指正。

目　录

前　言

第 1 章　信息安全保障基础 …… 1

1.1　信息安全保障背景 …… 1

1.1.1　信息安全的内涵和外延 …… 1

1.1.2　信息安全问题根源 …… 4

1.1.3　信息技术与信息安全发展阶段 …… 4

1.2　信息安全保障概念与模型 …… 6

1.2.1　信息安全保障概念 …… 6

1.2.2　信息安全保障相关模型 …… 7

1.3　信息系统安全保障概念与模型 … 12

1.3.1　信息系统安全保障概念 … 12

1.3.2　信息系统安全保障模型 … 14

思考题 …… 18

第 2 章　信息安全保障实践 …… 19

2.1　信息安全保障现状 …… 19

2.1.1　国外信息安全保障现状 … 19

2.1.2　我国信息安全保障现状 … 24

2.2　我国信息安全保障工作主要内容 …… 33

2.2.1　信息安全标准化 …… 33

2.2.2　信息安全应急处理与信息通报 …… 34

2.2.3　信息安全等级保护 …… 37

2.2.4　信息安全风险评估 …… 39

2.2.5　灾难恢复 …… 42

2.2.6　人才队伍建设 …… 43

2.3　信息安全保障工作方法 …… 44

2.3.1　确定信息安全需求 …… 45

2.3.2　设计并实施信息安全方案 … 46

2.3.3　信息安全测评 …… 46

2.3.4　信息安全监测与维护 …… 50

思考题 …… 50

第 3 章　信息安全管理基础 …… 51

3.1　信息安全管理概述 …… 51

3.1.1　信息安全管理基本概念 … 51

3.1.2　信息安全管理作用 …… 52

3.1.3　信息安全管理关键成功因素 …… 54

3.2　信息安全管理方法与实施 …… 55

3.2.1　信息安全管理方法 …… 55

3.2.2　信息安全管理实施 …… 57

思考题 …… 60

第 4 章　信息安全风险管理 …… 61

4.1　信息安全风险管理基础 …… 61

4.1.1　风险相关基本概念 …… 61

4.1.2　信息安全风险管理概述 … 63

4.1.3　信息安全风险相关政策与标准 …… 64

4.2　信息安全风险管理主要内容 …… 66

4.2.1 信息安全风险管理的基本内容和过程 …… 66
4.2.2 信息系统生命周期与信息安全风险管理 …… 68
4.3 信息安全风险评估主要内容 …… 70
4.3.1 风险评估工作形式 …… 70
4.3.2 风险评估方法 …… 71
4.3.3 风险评估的实施流程 …… 74
4.3.4 风险评估工具 …… 78
思考题 …… 79

第 5 章 信息安全管理体系 …… 80

5.1 信息安全管理体系基础 …… 80
5.1.1 管理职责 …… 80
5.1.2 文档控制 …… 81
5.1.3 内部审核和管理评审 …… 82
5.1.4 信息安全管理体系认证 …… 83
5.2 信息安全管理体系建设 …… 83
5.2.1 规划与建立 ISMS …… 83
5.2.2 实施和运行 ISMS …… 85
5.2.3 监视和评审 ISMS …… 86
5.2.4 保持和改进 ISMS …… 88
5.3 信息安全控制措施 …… 89
5.3.1 安全方针 …… 89
5.3.2 信息安全组织 …… 90
5.3.3 资产管理 …… 91
5.3.4 人力资源安全 …… 92
5.3.5 物理和环境安全 …… 94
5.3.6 通信和操作管理 …… 96
5.3.7 访问控制 …… 101
5.3.8 信息系统获取、开发和维护 …… 104
5.3.9 符合性 …… 106
思考题 …… 108

第 6 章 应急响应与灾难恢复 …… 109

6.1 应急响应概况 …… 109
6.1.1 信息安全事件分类与分级 …… 111
6.1.2 信息安全应急响应管理过程 …… 112
6.1.3 计算机取证 …… 114
6.2 信息系统灾难恢复 …… 115
6.2.1 灾难恢复概况 …… 115
6.2.2 灾难恢复管理过程 …… 119
6.2.3 灾难恢复能力 …… 122
6.3 灾难恢复相关技术 …… 123
6.3.1 存储技术 …… 124
6.3.2 备份技术 …… 125
6.3.3 备用场所 …… 126
6.3.4 云灾备技术 …… 128
6.4 灾难恢复案例 …… 128
6.4.1 灾难恢复需求分析 …… 129
6.4.2 灾难恢复策略制定 …… 130
思考题 …… 131

第 7 章 信息内容安全 …… 132

7.1 信息内容安全基础 …… 132
7.1.1 信息内容安全的内涵与界定 …… 132
7.1.2 信息内容安全与网络舆情 …… 133
7.1.3 网络舆情基本概念 …… 133
7.2 我国网络舆情状况 …… 134
7.2.1 网络舆情相关政策 …… 134
7.2.2 我国网络舆情生态 …… 136
7.3 网络舆情管理 …… 139
7.3.1 网络舆情收集 …… 139
7.3.2 网络舆情分析 …… 143
7.3.3 网络舆情应对 …… 145
思考题 …… 147

第 8 章 信息安全工程基础 …… 148

8.1 信息安全工程概述 …… 148

8.1.1 信息安全工程概念 …… 148
8.1.2 信息安全工程理论基础 … 149
8.2 信息安全工程实施 …… 153
8.2.1 发掘信息保护需求 …… 154
8.2.2 定义信息系统安全要求 … 155
8.2.3 设计系统安全体系结构 … 155
8.2.4 开发详细安全设计 …… 156
8.2.5 实现系统安全 …… 157
8.2.6 评估信息保护的有效性 … 158
8.2.7 支持认证和认可 …… 158
8.3 信息安全工程监理 …… 159
8.3.1 信息安全工程监理概述 … 159
8.3.2 工程招标阶段监理 …… 161
8.3.3 工程设计阶段监理 …… 163
8.3.4 工程实施阶段监理 …… 164
8.3.5 工程验收阶段监理 …… 165
思考题 …… 166

第 9 章 信息安全工程能力评估 …… 167

9.1 SSE-CMM 概述 …… 167
9.1.1 SSE-CMM 概念及作用 … 167
9.1.2 SSE-CMM 的体系结构 … 168
9.2 信息安全工程过程 …… 171
9.2.1 风险过程领域 …… 171
9.2.2 工程过程领域 …… 172
9.2.3 保证过程领域 …… 176
9.3 信息安全工程能力 …… 178
9.4 SSE-CMM 评估方法 …… 182
思考题 …… 183

第 10 章 信息安全法规与政策 …… 184

10.1 信息安全法规 …… 184
10.1.1 我国信息安全法规体系框架 …… 184
10.1.2 信息安全相关国家法律 …… 187
10.1.3 信息安全相关行政法规和部门规章 …… 196
10.1.4 信息安全相关地方法规、地方规章和行业规定 … 198
10.1.5 国外典型国家信息安全相关法规简介 …… 199
10.2 信息安全政策 …… 200
10.2.1 国家信息安全政策概况 … 200
10.2.2 信息安全相关国家政策 … 201
10.2.3 国外信息安全相关政策 … 209
思考题 …… 210

第 11 章 信息安全标准 …… 211

11.1 信息安全标准基础 …… 211
11.1.1 标准的作用 …… 212
11.1.2 标准化的特点和原则 … 213
11.1.3 我国国家标准的类型和代码 …… 214
11.1.4 标准的编制过程 …… 214
11.2 信息安全标准化组织 …… 215
11.2.1 国际信息安全标准化组织 …… 215
11.2.2 国外信息安全标准化组织 …… 217
11.2.3 我国信息安全标准化组织 …… 219
11.3 信息安全标准体系 …… 220
11.3.1 我国信息安全标准体系 …… 220
11.3.2 信息安全等级保护标准体系 …… 221
11.3.3 国际信息安全标准体系 … 223
11.4 我国信息安全典型标准介绍 … 223
11.4.1 基础标准 …… 224
11.4.2 技术与机制标准 …… 224

11.4.3 管理标准 …… 225
11.4.4 测评标准 …… 226
11.4.5 密码技术标准 …… 227
11.4.6 保密技术标准 …… 228
思考题 …… 228

第 12 章 信息安全道德规范 …… 229

12.1 信息技术通行道德规范 …… 229
12.1.1 计算机使用道德规范 … 229
12.1.2 互联网使用道德规范 … 230
12.2 信息安全从业人员道德规范 … 230
12.2.1 信息安全从业人员基本道德规范 …… 230
12.2.2 CISP 职业道德准则 …… 231
思考题 …… 232

附录 A 我国法律涉及信息安全条款摘录 …… 233
附录 B 部分信息安全国家标准列表 …… 253
附录 C 缩略语 …… 259
参考资料 …… 266

第 1 章

信息安全保障基础

阅读提示 本章主要介绍信息安全保障背景、概念与模型等方面的内容，使读者理解信息安全问题产生的根源，信息安全的内涵与外延，以及各个发展阶段的特点，了解 P2DR、IATF 等信息安全保障相关模型的基本思想和原理，掌握信息系统安全保障模型的保障目标、保障周期和保障要素。

1.1 信息安全保障背景

进入 20 世纪下半叶，信息技术飞速发展，成为最活跃的生产力要素，促使生产模式发生重大变革，引发了全球信息化浪潮。这场信息化浪潮的特点是利用信息技术，开发信息资源，促进信息交流，推动知识的传播与共享，加快了经济增长，从而推进社会发展转型。进入 21 世纪，经济全球化浪潮席卷各国，信息化成为经济全球化的倍增器，对经济发展、政府治理、社会变革、文化激荡、军事变革都起到了巨大的推动作用。随着信息化在国家发展中的重要性和地位的不断上升，信息安全事件不断增多，所造成的后果日益严重，信息安全逐渐得到国家重视。

1.1.1 信息安全的内涵和外延

信息安全是一门涉及计算机科学、网络技术、通信技术和密码技术等多个领域的交叉学科，它关注信息系统在安全方面存在的问题和面临的威胁，贯穿于信息系统中信息生命周期的整个过程。

1. 信息与信息安全

信息是有意义的数据，同其他重要的商业资产一样，是具有价值、需要适当保护的一种资产。信息可以以多种方式存在，可以打印或书写在纸张上，以电子文档或其他电子化形式存储及传播。信息及其所处环境如图 1-1 所示。如今信息已经成为组织的核心资产之一，保护信息安全需要从保护信息载体，乃至载体所处的环境着手。

图 1-1 信息及其所处环境

在ISO/IEC[⊖]27000《信息安全管理体系概述和术语》中，信息安全是指保持信息的保密性、完整性、可用性，有时也包括真实性、可核查性、不可否认性和可靠性等。信息安全的目标是保证信息的一系列安全属性得到保持、不被破坏，从而达到对组织业务运营能力的支撑作用。信息安全是一个广泛而抽象的概念，关注的是信息自身的安全。信息安全的任务是保护信息资产（信息及信息系统）免受未经授权的访问使用、披露、破坏、修改、查看、记录及销毁。信息本身应具有的安全属性主要有3个方面。

- 保密性：信息不泄露给未授权的访问者、实体和进程，或被其利用。
- 完整性：信息在存储或者传输过程中保持未经授权不能改变的特性，即对抗主动攻击，保持数据一致，防止数据被非法用户修改和破坏。
- 可用性：信息可被授权者访问并按需求使用的特性，即保证合法用户对信息和资源的使用不会被不合理地拒绝。

信息的以上3个基本安全属性习惯上简称为CIA（Confidentiality-Integrity-Availability）。

2. 特征与范畴

与传统安全相比，信息安全有4个鲜明特征：系统性、动态性、无边界性和非传统性。

（1）信息安全是系统的安全

信息安全问题是复杂的。信息化发展以巨大的力量推动着人类社会生存方式的重大变革，这一变革使我们面对前所未有的复杂环境：一个无所不在、全球互连互通的国际化网络空间，无数广域覆盖的、大规模复杂专用网络信息系统，品种多样的海量计算设备与信息处理终端。在这个“人－机”、“人－网”紧密结合的复杂系统中，某一分支或某一要害受到损害，均可能引发全局性的系统危机。从这个角度而言，我们不能孤立地从单一维度或者单个安全因素来看待信息安全，也不能将之视为单纯的技术问题或者管理问题，而是要系统地从技术、管理、工程和标准法规等各层面综合保障信息安全。

（2）信息安全是动态的安全

信息安全问题具有变化性。首先，信息系统从规划设计，到集成实施，再到运营维护，最后到废弃，在整个生命周期中，信息系统面临着不同的安全问题，因此不能用固化的视角看待。其次，信息系统所面临的风险是动态变化的，新的漏洞和攻击手段都会对系统的安全状况产生影响。此外，云计算、物联网、大数据和移动互联网等新技术在带给人们便利的同时，也产生了各种新的威胁和安全风险。综上所述，对信息安全不能抱有一劳永逸的思想，而是应该根据风险的变化，在信息系统的整个生命周期中采取相应的安全措施来控制风险。

信息安全的动态特性决定了信息安全问题与实践密切相关。信息安全已经从病毒传播、黑客入侵、技术故障等局部性、个别性和偶发性的问题，逐步转变为网络犯罪、网络恐怖主义等全球性的普遍问题，成为攻守双方在高新技术领域内展开的一场激烈较量。

（3）信息安全是无边界的安全

互联网是一个全球互连互通的国际化网络空间。信息化的重要特点是开放性和互通

⊖ 国际电工委员会（International Electrotechnical Commission，IEC）。

性，信息关键基础设施都是广域覆盖的大规模复杂信息系统，与互联网通过各种方式连接，例如金融、税务、电子政务系统等。同时，各系统之间也逐步实现互连互通，这使得信息安全威胁超越了现实地域的限制。此外，互联网具有传播速度快、覆盖面广、隐蔽性强和无国界等特点，违法犯罪活动不断向互联网渗透，这对信息安全保障提出了更高的要求。

（4）信息安全是非传统的安全

与军事安全、政治安全等传统安全相比，信息安全涉及的领域和影响范围十分广泛。如果信息安全得不到保障，虽然国家没有受到武力攻击，没有明确的敌对国家，领土和主权是完整的，但人们却感受到威胁的存在。传统维护安全的军事和治安手段无法应对信息安全问题，必须采用新方法来治理信息与互联网安全。

第一，信息安全是一个技术问题，如设备故障、系统本身存在的安全漏洞、系统配置不合理和黑客攻击等。互联网时代信息分布在网络中，大数据技术使信息的收集和整理变得越来越便捷，个人及单位信息容易暴露在网络中，网络泄密、窃密等现象严重，有效的安全技术措施是保护信息安全最直接的手段。

第二，信息安全是一个组织管理问题。信息安全的最终目标是保障信息系统所承载业务的安全。业务的引入使信息安全不仅仅是技术问题，它是人、技术系统和组织内部环境等综合因素产生的问题。对于组织而言，一方面，信息化促进了组织的工作效率提高、业务处理流程改进和人力成本降低，有效提升了组织的竞争力和效益；另一方面，由于业务日益依赖信息技术，技术故障、网络攻击和违规操作等给业务带来的损失也日益突出，极端情况下所造成的信息丢失和破坏甚至可能影响到组织的生存与发展。有效的信息安全管理能弥补单纯技术手段的不足。

第三，信息安全问题常常波及公众，社会影响面广。网络已经成为一种与报纸、电视等传统传媒共存的新兴传媒，并以其及时性、互动性等特有的优点，发挥着其他传媒所不具备的作用。网络的这个特点，使得网络成为民情汇聚之处、舆论汇聚之处、网民沟通之处。网络对社会稳定起着放大器的作用。一方面，网络是问政于民的有效手段，另一方面，网络也会将社会热点事件的影响快速扩散放大，如不能及时有效应对，容易造成群体事件，影响社会稳定。网络的普及，对政府治理提出了更高的要求，通过网络舆论手段，弘扬健康网络文化，培养良好的网络环境，将有助于形成良好的社会道德风尚。

第四，信息安全问题关系到社会稳定和国计民生，危及军事、经济等领域安全。当前关键基础设施广泛使用信息技术，尤其是交通运输、水利、供水、核设施、能源（包括电力、石油化工）和钢铁等工业控制领域，信息技术成为提高生产效率的核心手段。这些关键基础设施的工业控制系统一旦遭受安全攻击，将给人们生产生活造成严重影响。此外，网络攻击也日益成为国家之间外交纠纷的来源。各国已将其作为国家安全的组成部分，建立危机处理机制，加强互联网管控，通过法律手段打击网络犯罪，从源头上遏制网络犯罪蔓延势头。

1.1.2 信息安全问题根源

技术故障、黑客攻击、病毒和漏洞等原因都可以引发信息安全问题，信息安全问题产生的根源可以从内因和外因两个方面加以分析。

内因是信息系统自身存在脆弱性。信息系统过程、结构和应用环境的复杂性导致系统本身不可避免地存在脆弱性。换句话说，信息系统的脆弱性是一种客观存在。信息系统生命周期的各个阶段都可能引入安全缺陷。在需求分析和设计阶段，由于用户对安全重视不足，安全需求不明确，开发人员在设计过程中会优先考虑系统功能、易用性、代码大小和执行效率等因素，将安全放在次要位置。在实现阶段，尚未普遍使用软件安全开发工程，开发的软件存在安全缺陷。在使用和运行阶段，安全管理不到位，运维人员意识薄弱或能力不足，容易导致系统操作失误，或被恶意攻击。

外因是信息系统面临着众多威胁。这些威胁包括人为因素和非人为因素（也称为环境因素）两大类。人为因素可以分为个人威胁、组织威胁和国家威胁 3 个层面，根据掌握的资源，这 3 个层面所具备的威胁能力依次递增，如表 1-1 所示。非人为因素（如雷击、地震、火灾和洪水等自然灾害及极端天气）也容易引发信息安全问题。

表 1-1 外部威胁——人为因素

威胁的层面	威胁实施者	威胁手法
国家威胁	信息作战部队	巩固战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事、经济等情报信息
组织威胁	网络恐怖分子	破坏公共秩序、制造社会混乱等
	工业间谍	掠夺竞争优势、打击竞争对手
	网络犯罪团伙	获取非法经济利益等
个人威胁	社会型黑客	获取经济利益、恐吓、获取声望等
	娱乐型黑客	恶作剧、实现自我挑战等

1.1.3 信息技术与信息安全发展阶段

日益增加的信息化需求，愈演愈烈的信息安全事件，使信息安全技术和管理的概念不断发展深化，驱动人们对信息安全的认识也逐步加深。从最初关注通信安全发展到目前关注信息系统基础设施的信息保障，信息安全伴随着信息技术的变化而不断发展。

1. 信息技术发展阶段

人类进行通信的历史悠久。早在远古时期，人们就开始通过简单的语言等方式交换信息。随着文字的诞生，几千年来，书信一直是人们远程通信的主要手段。19 世纪中叶以后，随着电磁技术的发展，诞生了电报和电话，人类通信手段有了飞跃，开始进入新时代。1837 年，美国人摩尔斯（Morse）发明了电报机，将信息转换成电脉冲传向目的地，到达目的地后再转换为原来的信息，从而实现了长途电报通信。1875 年，贝尔发明了电话机。他于 1878 年在相距 300 公里的波士顿和纽约之间进行了首次长途电话实验，获得了成功。1906 年，美国物理学家费森登成功地研究出无线电广播。法国人克拉维尔建立了英法第一条商用无线电线路，推动了无线电技术的进一步发展。进入 20 世纪，尤其是在第二次世界

大战时期，军事和外交方面的巨大需求，使得无线通信技术得到飞速发展，用于传递军事情报、作战指令和外交政策等各种关键信息。

20 世纪发明的计算机，极大地改变了信息处理方式和效率，信息技术从此进入计算机阶段。1946 年，美国研制出电子数字积分计算机（Electronic Numerical Integrator And Computer，ENIAC），标志着数字电子计算机的诞生。ENIAC 重 30 吨，用了 18 000 个电子管。计算机经历了电子管、晶体管、集成电路（Integrated Circuit，IC）等阶段。20 世纪 70 年代，随着个人计算机的普及，人们开始使用计算机处理各种业务。计算机在处理、存储信息数据等方面应用越来越广泛。

计算机网络，尤其是互联网的出现，是信息技术发展历程中的一个里程碑事件，它将通信技术和计算机技术结合起来。在网络阶段，安全需求的核心是实现信息资产生成、处理、传输和存储等各阶段的保密性、完整性和可用性。

随着网络的普及，人们的工作、生活和学习已经越来越离不开网络，国家的经济发展和社会治理也都依赖网络。“网络空间”（Syberspace）成为与现实社会相对应的虚拟社会，进入网络化社会阶段，这个阶段的特征是各行业、各组织的业务越来越依赖于网络。信息技术的发展，对个人、组织、经济发展、社会稳定和国家安全都产生了巨大影响。

2. 信息安全发展阶段

人们对信息技术各个发展阶段涌现出的信息安全问题进行了探索与研究，以对抗各个阶段的威胁。信息安全的发展经历了通信安全（Communication Security，COMSEC）、计算机安全（Computer Security，COMPUSEC）、信息系统安全（Information Systems Security，INFOSEC）和信息安全保障（Information Assurance，IA）4 个阶段。

在通信安全阶段，信息安全主要面临的威胁是攻击者对通信内容的窃取。有线通信容易被搭线窃听，无线传播由于电磁波在空间传播易被监听。这使得保密成为通信安全阶段的核心安全需求。因此，这一阶段主要是通过密码技术加密通信内容，保证数据的保密性和完整性。

进入 20 世纪 70 年代，美国国家标准局（National Bureau of Standards，NBS）公布了《数据加密标准》（Data Encryption Standard，DES），标志着信息安全由通信保密阶段进入计算机安全阶段。这个时期，计算机网络尚未大规模普及。计算机阶段的主要威胁来自非授权用户对计算资源的非法使用，以及对信息的非授权修改和破坏。计算机安全的主要目的是确保信息系统的保密性、完整性和可用性，典型的安全措施是通过操作系统的访问控制技术来防止非授权用户的访问。1985 年，美国国防部（Department of Defense，DoD）发布《可信计算机系统评估准则》(Trusted Computer System Evaluation Criteria，TCSEC)，将操作系统安全分级。后来，安全方面的评估准则发展为彩虹系列。

信息系统安全也称网络安全，主要是保护信息在存储、处理和传输过程中免受非授权访问，防止授权用户遭受拒绝服务，同时检测、记录和对抗此类威胁。为了抵御这些威胁，人们开始使用防火墙、防病毒工具、公钥基础设施（Public Key Infrastructure，PKI）和虚拟专用网（Virtual Private Network，VPN）等安全产品。此阶段的主要标志是发布了《信息技术安全性评估通用准则》，此准则即通常所说的通用准则（Common Criteria，CC），后

转变为国际标准 ISO/IEC 15408。我国等同采纳此国际标准为国家标准 GB/T 18336。

1996 年美国国防部第 5-3600.1 号指令（DoDD 5-3600.1）第一次提出了信息安全保障（也称“信息保障”）的概念。当信息化从网络阶段进入网络空间阶段后，信息安全威胁来源从个人上升到犯罪组织，甚至国家力量。在这个阶段，人们认识到信息安全保障不能仅仅依赖于技术措施，开始意识到管理的重要性和信息系统的动态发展性，信息安全保障的概念逐渐形成和成熟。信息安全保障把信息安全从技术扩展到管理，从静态扩展到动态，通过技术、管理和工程等措施的综合融合，形成对信息、信息系统乃至业务使命的保障。

信息安全每个阶段所面临的典型威胁不断发生变化，每个阶段所采取的安全措施也有所不同，如表 1-2 所示。

表 1-2 信息安全发展各阶段

阶　段	年　代	典型威胁	安全措施
通信安全	20 世纪 40 ~ 70 年代	搭线窃听、密码学分析	加密
计算机安全	20 世纪 70 ~ 80 年代	非法访问、恶意代码等	安全操作系统技术
信息系统安全	20 世纪 90 年代	技术故障、网络入侵、病毒破坏等	防火墙、防病毒工具、漏洞扫描、入侵检测、PKI、灾难恢复等
信息安全保障	今天……	黑客、恐怖分子、信息战、自然灾难等	技术、管理、工程、人员培训等

进入 21 世纪后，尤其是从 2008 年起，在美国带动下，世界各国信息安全政策、技术和实践发生明显变革，纷纷将网络安全问题上升到国家安全的高度。2008 年 1 月，美国发布《国家网络安全综合倡议》（Comprehensive National Cybersecurity Initiative，CNCI），号称网络安全“曼哈顿项目”，提出网络威慑概念。2009 年 5 月 29 日美国发布《网络空间政策评估：确保信息和通讯系统的可靠性和韧性》报告。与信息安全保障相比，新的发展趋势是强调“威慑”概念，将防御、威慑和利用结合成三位一体的信息安全保障 / 网络空间安全（Information Security/Cyberspace Security，IA/CS）。

1.2 信息安全保障概念与模型

信息技术发展到网络化社会阶段，信息安全作为一个日益重要而尖锐的问题，涉及面越来越宽，众多因素和变量均处于“不确定”状态，在这种情况下只能维持一种动态、可控的安全状态，信息安全保障就是这样一种安全理念。

1.2.1 信息安全保障概念

为了满足现代信息系统和应用的安全保障需求，除了防止信息泄露、修改和破坏，还应当检测入侵行为；计划和部署针对入侵行为的防御措施；同时，采用安全措施和容错机制，在遭受攻击的情况下，保证机密性、私密性、完整性、抗抵赖性、真实性、可用性和可靠性；修复信息和信息系统所遭受的破坏。这被称作“信息安全保障”，它能够不受安全威胁的影响，在分布式和不同种类计算和通信环境中，传递可信、正确、及时的信息。通

过保证信息和信息系统的可用性、完整性、保密性及抗抵赖性来保护信息和信息系统，包括通过综合保护、检测和响应等能力为信息系统提供修复。

同传统的信息安全和信息系统安全的概念比较，不难看出信息安全保障的概念更加广泛。首先，传统信息安全的重点是保护和防御，而信息安全保障的概念是保护、检测和响应的综合。其次，传统信息安全的概念不太关注检测和响应，但是信息安全保障非常关注这两点。再次，攻击后的修复不在传统信息安全概念的范围之内，但是它是信息安全保障的重要组成部分。最后，传统信息安全的目的是为了防止攻击的发生，而信息安全保障的目的是为了保证当有攻击发生时，信息系统始终能保证维持特定水平的可用性、完整性、真实性、机密性和抗抵赖性。

毋庸置疑，信息安全保障包含许多学科，有多种方面，如策略、法规、道德、管理、评估和技术。同传统的信息安全实践相比，信息安全保障不仅包含设计和改进各种新安全技术，还包括多种应急策略、法规、道德、社会、经济、管理、评估和保障问题，信息安全保障加快了人们对信息安全实践的步伐。

1.2.2 信息安全保障相关模型

信息安全保障相关模型能准确描述安全的重要方面与系统行为的关系，提高对成功实现关键安全需求的理解层次，“计划 – 执行 – 检查 – 改进”（Plan Do Check Act，PDCA）模型和信息保障技术框架是信息安全管理和信息安全保障技术实施过程遵循的方法和思想。

1. P2DR 模型

防护 – 检测 – 响应（Protection Detection Response，PDR）模型的基本思想是承认信息系统中存在漏洞，正视系统面临的威胁，通过适度防护并加强检测，落实安全事件响应，建立威胁源威慑，保障系统安全。该模型认为，任何安全防护措施都是基于时间的，超过该时间段，这种防护措施就可能被攻破。该模型给出了信息系统攻防时间表，攻击时间指的是系统采取某种防守措施，使用不同的攻击手段攻破该防守措施所需要的时间。防守时间指的是对于某种固定攻击采取不同的安全防护措施，该防护措施所能坚守的时间。PDR 模型直观、实用，但对系统的安全隐患和安全措施采取相对固定的假设前提，难以适应网络安全环境的快速变化。

在 PDR 模型基础上，增加策略要素便形成了“策略 – 防护 – 检测 – 响应”（Policy Protection Detection Response，P2DR/PPDR）模型，即“策略 – 防护 – 检测 – 响应”。该模型的核心是信息系统所有防护、检测和响应都是依据安全策略实施的，如图 1-2 所示。

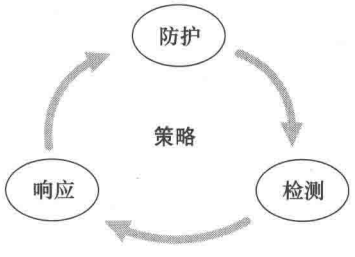

图 1-2 P2DR 模型

在 P2DR 模型中，策略指信息系统的安全策略，包括访问控制、加密通信、身份认证和备份恢复等，策略体系的建立包括安全策略的制订、评估与执行等。防护指通过部署和采用安全技术来提高信息系统的防护能力，如访问控制、防火墙、入侵检测、加密和身份认证等技术。检测指利用信息安全检测工具，监视、分析、

审计网络活动，了解信息系统的安全状态。检测使安全从被动防护演进为主动防御，体现了模型的动态性，主要方法包括实时监控、检测和报警等。响应指检测到安全漏洞和事件时，及时通过响应措施将信息系统的安全性调整到风险最低的状态，其主要方法包括关闭服务、跟踪反击、消除影响、启动备份系统，以及恢复系统功能和数据等。

在P2DR模型中，可以将各个环节所需时间与防护时间相比较，判断信息系统在面临各种威胁时是否安全。假设系统S的防护、检测和响应时间分别是Pt、Dt和Rt，系统被对手成功攻击后的暴露时间为Et，那么可以根据下面两个关系式来判断系统S是否安全：

- 如果 $Pt > Dt + Rt$，那么S是安全的；
- 如果 $Pt < Dt + Rt$，那么 $Et = (Dt + Rt) - Pt$。

P2DR模型的核心思想是：在统一安全策略的控制下，综合运用防护工具，使用检测工具检测、评估系统的安全状态，及时通过响应措施将系统调整到安全风险最低的状态。

与PDR模型相比，P2DR模型更突出控制和对抗，即强调系统安全的动态性，并且以安全检测、漏洞监测和自适应填充“安全间隙”为循环来提高网络安全。P2DR模型还考虑了管理因素，强调安全管理的持续性，关注检测的重要性，通过实时监视网络活动，发现威胁和弱点来修补安全漏洞。

目前，P2DR模型又有了新的发展，形成“策略－防护－检测－响应－恢复”（Policy Protection Detection Response Recovery，P2DR2/PPDRR）模型。P2DR2是一种动态的、自适应的安全处理模型。在进行风险处理时可参考此模型，以适应安全风险和安全需求的不断变化，提供持续的安全保障。PPDRR模型包括策略、防护、检测、响应和恢复5个主要部分，防护、检测、响应和恢复构成一个完整的、动态的安全循环，在安全策略的指导下共同实现安全保障。不同等级的信息系统的安全保护要求不同，因而可采用不同的风险处理模型。对于安全保护等级为4及以上的信息系统，建议采用PPDRR，安全保护等级为3的信息系统，建议参考PPDRR模型，安全保护等级为2及以下的信息系统，可不做要求。

风险处理的需求来自机构信息系统的安全要求和风险评估结果。针对不同的风险处理需求，应采取不同的风险处理措施。表1-3根据PPDRR模型列出了主要的风险处理需求及其相应的风险处理措施。

表1-3 主要的风险处理需求及其相应的风险处理措施

PPDRR要素	风险处理需求	风险处理措施
策略（Policy）	设备管理制度	建立与健全各种安全相关的规章制度和操作规范，使得保护、检测和响应环节有章可循、切实有效
	机房出入守则	
	系统安全管理守则	
	系统安全配置明细	
	网络安全管理守则	
	网络安全配置明细	
	应用安全管理守则	
	应用安全配置明细	
	应急响应计划	
	安全事件处理准则	