教育部–华为产学合作协同育人项目规划教材

信息安全技术

(HCIA-Security)

刘洪亮 杨志茹 | 主编
向磊 刘洋 周思难 郭俊 | 副主编

- 教育部 – 华为产学合作协同育人项目成果
- 由企业与院校联合编写完成，可作为 HCIA 认证考试教材
- 以解决实际问题为学习目标，以完成实战案例为学习手段

INFORMATION SECURITY TECHNOLOGY

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

教育部-华为产学合作协同育人项目规划教材

信息安全技术

(HCIA-Security)

刘洪亮 杨志茹 | 主编
向磊 刘洋 周思难 郭俊 | 副主编

INFORMATION SECURITY TECHNOLOGY

人民邮电出版社
北京

图书在版编目（CIP）数据

信息安全技术 = HCIA-Security / 刘洪亮，杨志茹主编. -- 北京 : 人民邮电出版社，2019.4
教育部-华为产学合作协同育人项目规划教材
ISBN 978-7-115-50380-0

Ⅰ. ①信… Ⅱ. ①刘… ②杨… Ⅲ. ①信息安全－安全技术－教材 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2019)第038806号

内 容 提 要

本书是面向华为安全认证体系的教材。书中以华为 HCIA-Security 认证考试内容为对象，详细讲述了当前信息安全技术相关的各方面知识，内容包括信息安全基础概念、信息安全规范简介、网络基本概念、常见网络设备、常见信息安全威胁、威胁防范与信息安全发展趋势、操作系统简介、常见服务器种类与威胁、主机防火墙和杀毒软件、防火墙介绍、网络地址转换（NAT）技术、防火墙双机热备技术、防火墙用户管理、入侵防御简介、加密与解密原理、PKI 证书体系、加密技术应用、安全运营与分析基础、数据监控与分析、电子取证、网络安全应急响应、案例研讨等，涵盖了目前 HCIA-Security 认证考试体系的相关内容与技术。

本书可作为高等学校本、专科信息安全相关专业的教材，也可作为企事业单位网络信息安全管理人员入职与培训的参考书，还可以作为 HCIA-Security 考证培训用书。

◆ 主　　编　刘洪亮　杨志茹
副 主 编　向　磊　刘　洋　周思难　郭　俊
责任编辑　范博涛
责任印制　马振武

◆ 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
固安县铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：18.25　　2019 年 4 月第 1 版
字数：539 千字　　2019 年 4 月河北第 1 次印刷

定价：59.80 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 FOREWORD

进入 21 世纪，随着信息技术的不断发展，信息安全问题也日显突出。如何确保信息系统的安全已成为全社会关注的问题。国际上对信息安全的研究起步较早，投入力度大，已取得了许多成果，并得以推广应用。目前国内已有一批专门从事信息安全基础研究、技术开发、技术服务的研究机构与高科技企业，形成了我国信息安全产业的雏形，但由于国内专门从事信息安全工作的技术人才严重短缺，阻碍了我国信息安全事业的发展。

信息安全工程师专门解决这类问题，为客户保证信息和网络的基本安全，可以说是网络和信息安全的“医生”。信息安全工作需要整合计算机网络安全、操作系统安全、数据安全、密码学、安全运营等方面的知识和技能，其涉及的知识面广，实践性强。随着技术的发展，信息安全正在发展成为一个不可或缺的行业。

华为认证是华为技术有限公司（简称“华为”）凭借多年在信息通信技术领域的人才培养经验，基于 ICT 产业链的人才职业发展生命周期，以层次化的职业技术认证为指引，推出的覆盖 IP、IT、CT 及 ICT 融合技术领域的认证体系；它是 ICT 全技术领域的认证体系。

本书的编写融入了丰富的教学和实际工作经验，内容安排合理，组织有序。书中各章均为一个完整模块，由课程导入、相关内容、本章小结、技能拓展、课后习题等层次组成，让读者循序渐进地学习，并通过多个实际案例的精讲，激发读者的学习兴趣，帮助读者更快、更全面地掌握 HCIA-Security 认证的核心知识，并解决实际工作问题。

本书由刘洪亮、杨志茹主编，向磊、刘洋、周思难、郭俊为副主编，杨志茹编写第 1～3 章，郭俊编写第 4～6 章，向磊编写第 7～9 章，周思难编写第 10～14 章，刘洪亮编写第 15～18 章、刘洋编写第 19～22 章。

本书在编写的过程中得到了华为技术有限公司 ICT 学院、武汉誉天互联科技有限责任公司阮维的大力支持，在此一并表示感谢。

由于编者水平有限，书中难免有不足之处，敬请广大读者批评指正，以便在今后的修订中不断改进。编者联系邮箱 liuhlzz@21cn.com。

编者

2019 年 1 月

目录 CONTENTS

此为试读，需要完整PDF请访问：www.ertongbook.com

第11章

第12章

第13章

第14章

第15章

第16章

第17章

第18章

第19章

第20章

第21章

第22章

第1章 信息安全基础概念

01

知识目标

1. 了解信息安全的发展历史。
2. 了解信息安全的定义和特点。
3. 了解信息安全管理的重要性。

能力目标

1. 学会区分不同的安全风险。
2. 掌握每一种安全风险的特点。

课程导入

小华是华安公司的一名技术职员，随着互联网发展和 IT（Information Technology，信息技术）的普及，网络和 IT 已经日渐深入到工作和日常生活当中，信息网络化和社会信息化突破了应用信息在时间和空间上的障碍，使信息的价值不断提高，因此这也为小华日常工作提供了很多便利。但是与此同时，网页篡改、计算机病毒、系统非法入侵、数据泄露、网站欺骗、服务瘫痪、漏洞非法利用等信息安全事件时有发生。

相关内容

1.1 信息与信息安全

1.1.1 信息

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，由图 1-1 可知，信息包括书本信件、国家机密、电子邮件、雷达信号、交易数据、考试题目等。

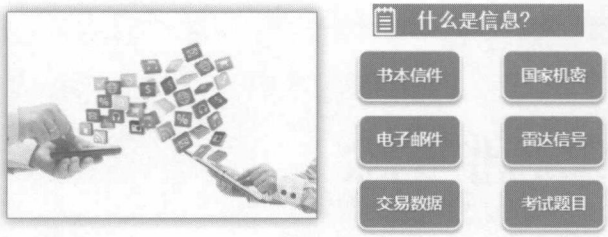

图 1-1　信息含义

1.1.2　信息安全

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。图 1-2 所示为信息安全的危害。

图 1-2　信息安全的危害

1.2　信息安全发展历程

1.2.1　信息安全发展的历史

信息安全发展历程如图 1-3 所示。

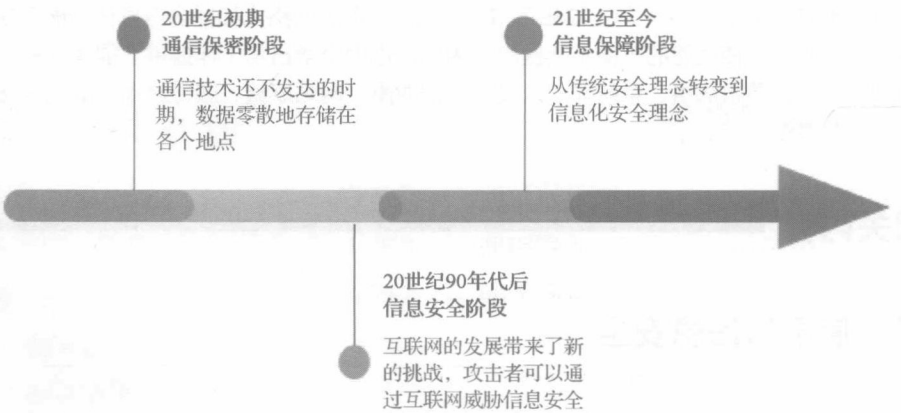

图 1-3　信息安全发展历程

1. 通信保密阶段

在通信保密阶段中通信技术还不发达，数据只是零散地存储在不同的地点，信息系统的安全仅限于保证信息的物理安全，以及通过密码（主要是序列密码）解决通信安全的保密问题。把信息安置在

相对安全的地点，不容许非授权用户接近，就基本可以保证数据的安全性了。

2. 信息安全阶段

从 20 世纪 90 年代开始，由于互联网技术的飞速发展，无论是企业内部还是外部信息都得到了极大的开放，而由此产生的信息安全问题也跨越了时间和空间，信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为诸如可控性、不可否认性等其他的原则和目标。具体如图 1-4 所示。

图 1-4　信息安全问题焦点转变

3. 信息保障阶段

从图 1-5 可知，进入面向业务的安全保障阶段后，可从多角度来考虑信息的安全问题。

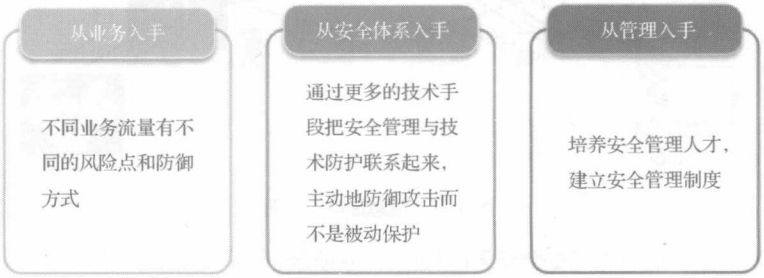

图 1-5　多角度考虑信息安全问题

1.2.2　信息安全涉及的风险

信息安全涉及的风险如图 1-6 所示。

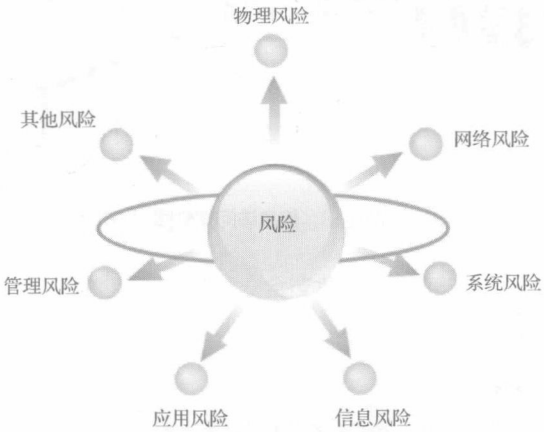

图 1-6　信息安全涉及的风险

1. 物理风险

① 设备被盗、被毁。

② 链路老化，人为破坏，被动物咬断等。

此为试读，需要完整PDF请访问：www.ertongbook.com

③ 网络设备自身故障。

④ 停电导致网络设备无法工作。

⑤ 机房电磁辐射。

2. 信息风险

① 信息存储安全。信息存储安全包括数据中心安全和组织安全，它需要满足各种数据库和应用的不同层次的安全需求原则。

② 信息传输安全。信息传输安全示意图如图 1-7 所示。

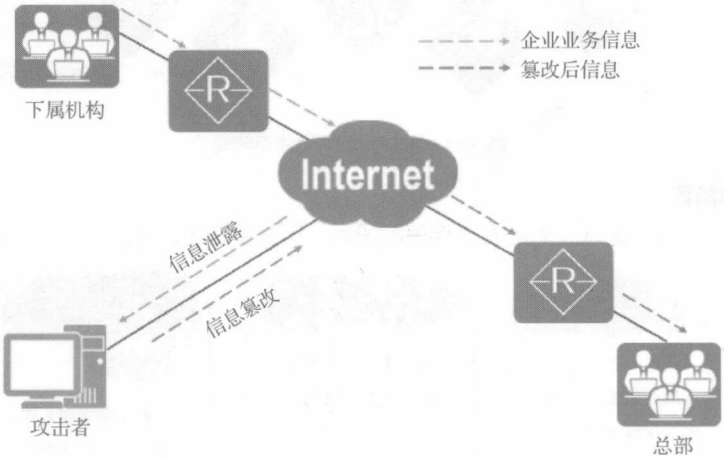

图 1-7　信息传输安全图

③ 信息访问安全。信息访问安全示意图如图 1-8 所示。

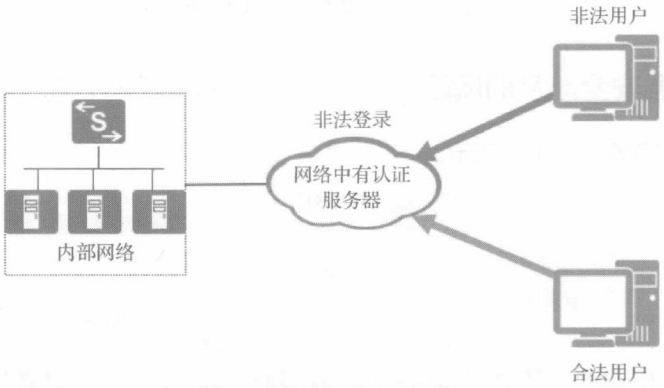

图 1-8　信息访问安全图

3. 系统风险

① 数据库系统配置安全。

② 系统存储数据的安全。

③ 系统中运行的服务安全。

4. 应用风险

① 网络病毒。

② 操作系统安全。

③ 电子邮件应用安全。

④ Web 服务安全。

⑤ FTP 服务安全。
⑥ DNS 服务安全。
⑦ 业务应用软件安全。

5. 网络风险

网络风险示意图如图 1-9 所示。

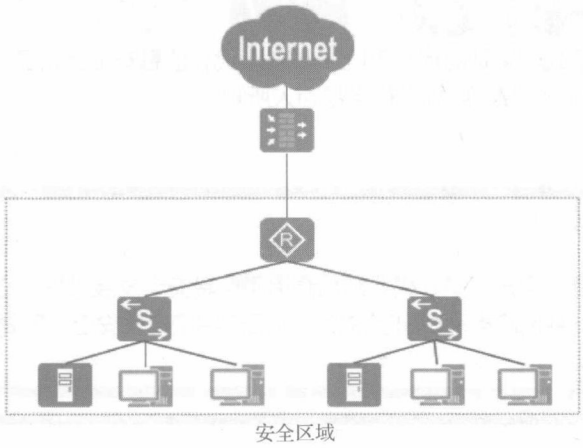

图 1-9　网络风险示意图

6. 管理风险

信息系统是否存在管理风险，可以从以下几个方面讨论。

① 国家政策：国家是否制定了健全的信息安全法规；国家是否成立了专门的机构来管理信息安全。

② 企业制度：企业是否制定了安全管理规则、责权分明的机房管理制度；企业是否建立了自己的安全管理机构。

③ 管理体系：是否明确了有效的安全策略、高素质的安全管理人员；是否有行之有效的监督检查体系，保证规章制度被顺利执行。

1.3 信息安全管理的重要性及发展现状

信息化越发展，信息安全越重要，信息网络成为经济繁荣、社会稳定和国家发展的基础。信息化深刻影响着全球经济的整合、国家战略的调整和安全观念的转变，信息安全已经从单纯的技术性问题变成事关国家安全的全球性问题。

1.3.1 信息安全管理的重要性

安全技术知识是信息安全控制的手段，要让安全技术发挥应有的作用，必然要有适当管理程序的支持。据统计，企业信息受到损失的 70%是由于内部员工的疏忽或有意泄露造成的，具体如图 1-10 所示。

图 1-10　造成信息泄露的主要因素

1.3.2 信息安全管理的发展现状

各个国家都已经制定了自己的信息安全发展战略和发展计划，确保信息安全正确的发展方向。主要有以下两方面。

（1）加强信息安全立法，实现统一和规范管理：以法律的形式规定和规范信息安全工作，是有效实施安全措施的最有利保证。

（2）步入标准化与系统化管理时代：20 世纪 90 年代，信息安全步入了标准化与系统化的管理时代，其中以 ISO/IEC 制定的 27000 标准体系最为人所知。

本章小结

本章先对信息与信息安全进行了介绍，然后介绍了信息安全发展过程，之后介绍了信息安全涉及的风险类别，并针对每一种风险类别做出了说明，最后介绍了信息安全的重要性及发展现状。

技能拓展

✧ 信息安全案例 1——WannaCry

2017 年，不法分子利用 Windows 系统黑客工具 EternalBlue（永恒之蓝）传播一种勒索病毒软件 WannaCry，超过 10 万台计算机遭到了勒索病毒攻击、感染，造成损失达 80 亿美元，如图 1-11 所示。

图 1-11 计算机遭勒索病毒攻击

✧ 信息安全案例 2——海莲花

2012 年 4 月起，某境外组织对政府、科研院所、海事机构、海运建设、航运企业等相关重要领域展开了有计划、有针对性的长期渗透和攻击，代号为 OceanLotus（海莲花）。意图获取机密资料，截获受害计算机与外界传递的情报，甚至操纵终端自动发送相关情报。图 1-12 所示为计算机遭受攻击的原因分析。

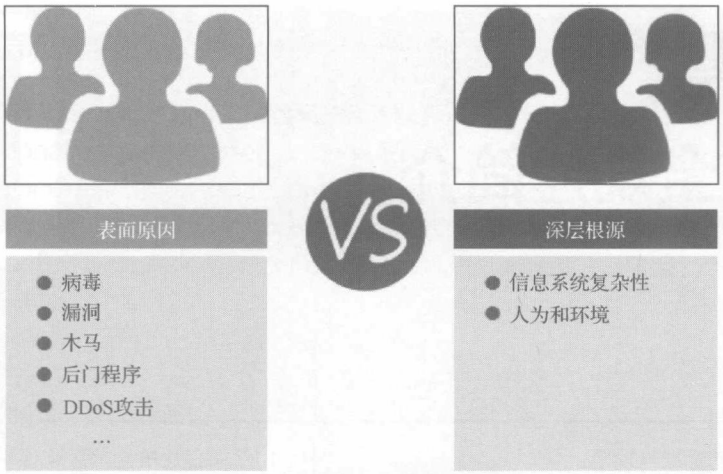

图 1-12　计算机遭受攻击的原因分析

课后习题

1. 信息安全事件频发的原因是存在漏洞、病毒、后门程序等安全攻击手段（　　）。
   A. 正确　　B. 错误
2. 信息安全的基本属性为（　　）。
   A. 保密性　　B. 完整性
   C. 可用性、可控性、可靠性　　D. 以上都是
3. 简述信息安全发展的历程。
4. 信息安全涉及的风险有哪些?
5. 信息安全风险中的信息风险包括哪些?

第 2 章 信息安全规范简介

02

知识目标

1. 了解信息安全的标准与规范。
2. 了解信息安全管理体系。
3. 了解信息安全等级化保护体系。

能力目标

1. 掌握常见信息安全标准。
2. 掌握信息安全标准的意义。
3. 掌握常见信息安全标准的主要内容。

课程导入

小安是华安公司的一名底层员工，平常对互联网的了解较少，接触也不多，总认为网络世界不太可靠，信息容易泄露，加上网络上信息泄露的事件层出不穷，更加使小安望而却步。但是，最近小安因为业务的发展，尝到了互联网的甜头，自己便有了对互联网进一步了解的愿望。因此，小安想知道什么是信息安全标准？信息安全的管理体系及规划是什么？而公司的技术员工小华将对其做一个详细的介绍。

相关内容

2.1 信息安全标准与组织

2.1.1 信息安全标准

信息安全标准是规范性文件之一，其定义是为了在一定的范围内获得最佳秩序，经协商一致制定并由公认机构批准，共同使用的和重复使用的一种规范性文件。

2.1.2 信息安全标准组织

在国际上，与信息安全标准化有关的组织主要有以下 4 个：
（1）International Organization for Standardization（ISO，国际标准化组织）
（2）International Electrotechnical Commission（IEC，国际电工委员会）
（3）International Telecommunication Union（ITU，国际电信联盟）
（4）The Internet Engineering Task Force（IETF，Internet 工程任务组）
国内的安全标准组织主要有：
（1）全国信息技术安全标准化技术委员会（CITS）
（2）中国通信标准化协会（CCSA）下辖的网络与信息安全技术工作委员会
常见信息安全标准与规范如图 2-1 所示。

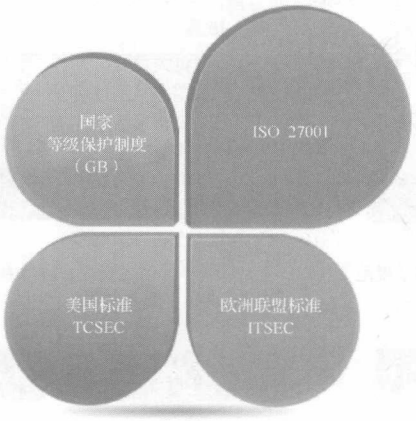

图 2-1 常见信息安全标准与规范

2.2 信息安全管理体系

信息安全管理体系（Information Security Management System，ISMS）的概念最初来源于英国标准学会制定的 BS 7799 标准，并伴随着其作为国际标准的发布和普及而被广泛地接受，具体如图 2-2 所示。

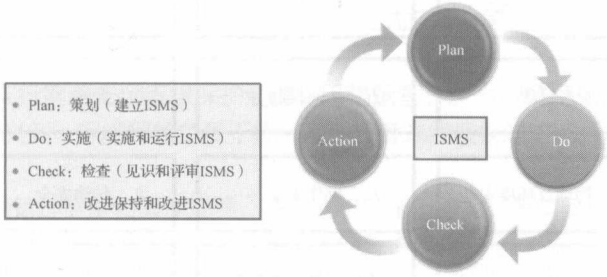

图 2-2 信息安全管理体系

2.2.1 ISO 27000 信息安全管理体系家族

ISO 27000 信息安全管理体系家族如图 2-3 所示。

此为试读，需要完整PDF请访问：www.ertongbook.com