信息安全保障人员认证培训教材

信息系统安全集成

XIN XI XI TONG AN QUAN JI CHENG

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 秦潇潇 万里冰 张 斌

★★★ CISAW ★★★

电子科技大学出版社

信息安全保障人员认证培训教材

信息系统安全集成

XIN XI XI TONG AN QUAN JI CHENG

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 秦潇潇 万里冰 张 斌

★★★ CISAW ★★★

电子科技大学出版社

图书在版编目（CIP）数据

信息系统安全集成 / 张剑主编. -- 成都：电子科技大学出版社，2015.5

ISBN 978-7-5647-2976-9

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息系统-安全集成-研究 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2015）第 082243 号

内 容 提 要

本书在《信息安全技术》基础课程重点阐述CISAW信息安全保障模型基础上，深入诠释了“安全的集成”和“集成的安全”的核心概念，独具特色地提出信息系统“安全集成”和“集成安全”的保障模式，并对模型中涉及的各环节进行全面论述并深入分析，提出了信息系统安全集成的初步理论构架。本书结合具体案例阐述模型中涉及的各项具体内容，建立信息系统安全集成项目的具体分析、设计、开发、集成实施、安全测评、安全提升与改进的业界参照流程。

信息系统安全集成

主　编　张　剑

副主编　秦潇潇　万里冰　张　斌

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

策划编辑：徐守铭

责任编辑：李　毅

主　　页：www.uestcp.com.cn

电子邮箱：uestcp@uestcp.com.cn

发　　行：新华书店经销

印　　刷：成都市川侨印务有限公司

成品尺寸：185 mm × 260 mm　　**印张** 12.25　　**字数** 270 千字

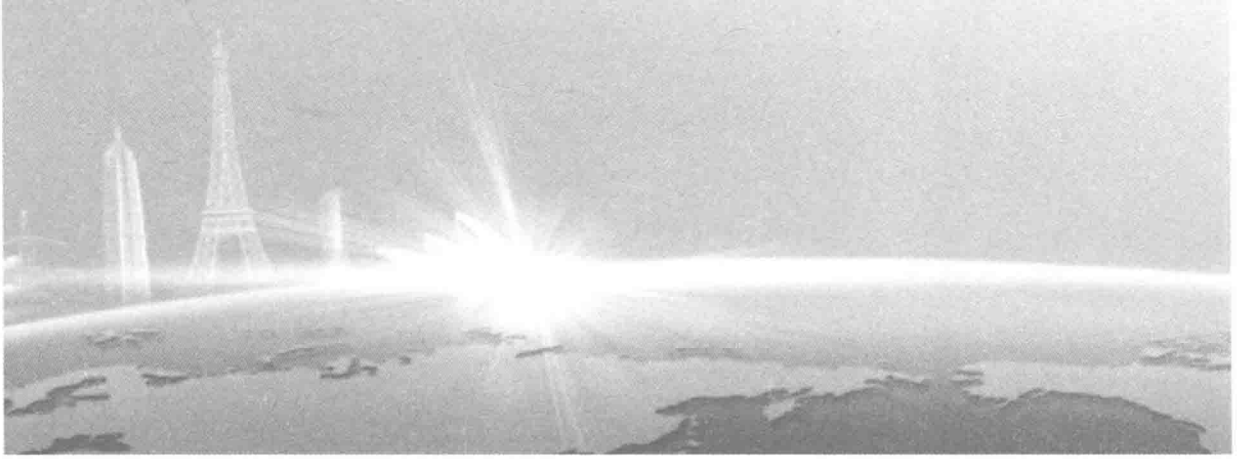
版　　次：2015 年 5 月第一版

印　　次：2015 年 5 月第一次印刷

书　　号：ISBN 978-7-5647-2976-9

定　　价：50.00 元

丛书编委会



编 写 组

主　编　张　剑

副主编　秦潇潇　万里冰　张　斌

编　委　杜孝伟　孙　敏　罗俊海　赵　洋　赵　辉

序

2014年，我国提出了建设网络强国战略与目标。实现网络强国，培养和造就网络与信息安全人才队伍是关键。据调查，截至2014年年底，国内网络与信息安全人才缺口高达50万人，并呈现持续增长的趋势。加快人才培养是我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。

作为我国专业信息安全认证机构和培训机构，中国信息安全认证中心以保障国家网络与信息安全为己任，于2011年推出了信息安全保障人员认证（CISAW）。CISAW认证是面向IT从业人员、在校学生，特别是与网络与信息安全密切相关的高级管理人员、专业技术人员推出的人员资格认证和专业水平认证。CISAW认证的推出和实施，为培养和造就我国网络与信息安全人才探索了一条有效途径，得到了业内专家和社会各界的好评。

推行CISAW认证，编写高质量的教材尤为重要。鉴于此，中国信息安全认证中心组织国内信息安全保障的专业技术和应用领域的专家，依据《信息安全保障人员认证考试大纲》要求，结合信息安全保障工作的各岗位知识和应用能力要求，共同编著了信息安全保障人员认证系列教材。本系列教材包括《信息安全技术》《信息安全技术应用》和《信息安全实验》3种基础教材；《软件安全开发》《信息系统安全集成》《信息安全管理》《信息安全咨询手册》《信息系统安全运维》《信息系统安全审计》《信息安全风险管理》《网络攻防技术》《业务连续性管理》《云计算安全》《物联网安全》和《工业控制安全》12种专业技术应用教材；《电子政务安全》《电子商务安全》《交通服务信息安全》《能源服务信息安全》《医疗卫生信息安

全》《教育服务信息安全》《金融服务信息安全》《通信服务信息安全》《宾馆服务信息安全》和《物流服务信息安全》10种应用领域教材。

本系列教材以实用为首要原则，从统一的信息安全保障模型出发，构建了包括信息安全技术基础知识、信息安全专业技术知识和应用领域安全保障管理知识的完整信息安全保障知识体系。既是广大CISAW认证申请者的考试指导用书，同时也是广大信息安全保障工作者的工作指南和参考用书。

希望本系列教材的出版，能为广大信息安全保障从业者学习、工作和申请认证提供指导和帮助。

是为序。

中国信息安全认证中心主任　魏　昊

2014年12月28日

前　言

2011 年，《信息系统安全集成》讲义开始印发使用。4 年中，讲义经过了多期培训班的交流和研讨，最终总结、积淀并形成了完整的知识体系，并以正式图书形式与读者见面。书中提出了信息系统安全集成模型，该模型是在 CISAW 信息安全保障统一模型的基础上推演而来。模型中同时总结出了“安全集成”和“集成安全”两种模式。本书以该模型和其中的两种模式为框架展开，因此，对该模型及其两种模式的理解将有助于对本书知识的学习和掌握。

本书共分为 6 章。第 1 章概述，从基本定义出发，重点介绍了本书的核心模型——信息系统安全集成模型；第 2 章信息系统安全工程综述，从安全集成基本理论的角度介绍了信息系统安全工程的概念、范畴等基本知识和方法；第 3 章安全集成工程实施，在前两章介绍基本理论和知识的基础上，结合信息系统安全集成过程，给出了信息系统安全工程具体的实施工作的指导；第 4 章和第 5 章在第 3 章的基础上，结合实际案例给出了“安全集成”和“集成安全”两种模式进行信息系统安全集成的工程实施过程与分析；最后，第 6 章为认证培训的学员对相关的服务资质认证标准进行了解读，以便于更好地理解认证标准要求和认证过程。

本书按照信息安全保障人员认证考试大纲的要求进行编写，适合广大申请认证考试的人员使用的同时，也适合所有从事与信息系统安全集成有关的工作人员、期望了解信息系统安全集成相关知识的人员使用。本书配套教程《信息安全技术》，详细介绍了相关信息安全技术的基本概念和技术

原理，可供相关人员参考。

本书由张剑、秦潇潇、万里冰、张斌、杜孝伟、孙敏、罗俊海、赵洋、赵辉等共同编写完成。

本书在成书过程中得到了《信息安全保障人员认证考试用书》编委会的指导和中国信息安全认证中心、四川省中认信安技术服务有限公司、四川亚和企业咨询服务有限公司的大力支持，在此表示衷心感谢。

本书力图以明确的思路、清晰的结构和流畅的语言来展现本书的知识体系，但难免会出现疏漏、差错和不足，在此，恳请广大读者和同行批评指正，以便我们再版修订时加以改正和完善。

张　剑

2014 年 12 月 31 日

目　录

第1章 概 述

随着我国信息化进程的推进，信息系统应用到社会的各个领域。信息及网络通信技术的进步为信息共享、数据融合、系统集约化提出了新的需求，信息系统在功能不断强大的同时，系统构成却越来越复杂，安全问题层出不穷。

信息社会发展过程中，新旧信息系统并存的现象将一直存在，如何实现对信息系统的安全集成是本书讨论的主要话题。

1.1 信息系统

对信息系统的理解需要从信息和系统两个基本概念入手。

1. 信息

长期以来，信息的定义一直是科学家讨论的话题。目前，关于信息的定义较多。

控制论创始人维纳（Norbert Wiener）认为："信息是人们在适应外部世界，并使这种适应反作用于外部世界的过程中，同外部世界进行互相交换的内容和名称。"

我国国家标准 GB4894—85《情报与文献工作词汇基本术语》中定义信息为："物质存在的一种方式、形态或运动形态，也是事物的一种普遍属性，一般指数据、消息中所包含的意义，可以使消息中所描述事件中的不定性减少。"

在现代科学中，信息指事物发出的消息、指令、数据、符号等所包含的内容。

本书对信息的定义采用香农（C. E. Shannon）博士 1948 年在《通信的数学理论》一文中，从数学的角度间接给出了信息的定义。他的定义可以描述为：信息是消除不确定性的东西。

我们认为，信息通过一定数据形式展现，这些数据是寄生于一定的存储和传输载体中的。信息作为一种实体对象，和自然界其他事物一样，有产生、发展和消亡的过程，即生命周期。信息的生命周期包括了信息的产生、存储、传输、处理和销毁等诸多环节。

2. 系统

关于系统，一般系统论创始人贝塔朗菲，认为："系统是相互联系相互作用的诸元素的综合体。"

我国著名科学家钱学森认为："系统是由相互作用相互依赖的若干组成部分结合而成的，具有特定功能的有机整体，而且这个有机整体又是它从属的更大系统的组成部分。"

辞海对系统作为名词给出了这样的解释："同类事物按一定的秩序和内部联系组合而成的整体"或"由要素组成的有机整体"。

GB/T20261《系统安全工程成熟度模型》中定义系统是"具有实物形式和规定目的的、可识别的离散实体；通过集成相互作用的部件构成，单独的每一个部件达不到所要求的总体目的"。

参考文献1中，定义系统（system）是："A system is a set of interacting or interdependent components forming an integrated whole"，即，系统是一组相互联系而又相互独立的组件所构成的一个整体。

朗文当代英语词典中定义系统为："A group of related parts that work together as whole for particular purpose"，即，一组相互关联的部件，它们作为一个整体共同工作以完成特定功能。

可见系统具有几个基本特征。

1）有机组合

系统都是由若干要素组成的，是有机组合在一起的，即组成要素之间存在特定的联系和相互作用。一般地，组合后的系统所发挥的功能超过其组成要素的单一功能的总和。

2）整体性和独立性

组合后的系统是一个有机的整体。整体性说明系统各组成要素的分割将导致系统功能的丧失。整体性的另一个方面说明系统具有相对的独立性。

3）层次性和聚合性

系统的构成部件有时也是一个系统，我们称之为子系统。因而，系统和部件是一个相对概念，不是绝对的。这与我们认识自然具有一致性，复杂的事物通常由简单的事物构成；复杂的系统通常由若干简单的子系统有机构成。

4）稳定性

在一段时间内，系统的组成是稳定的。这是符合事物的从量变到质变的发展规律的。经历一段时间的运转，系统构成将发生一定的改变，这意味着原有系统的更新和升级，或者我们称之为进化。

3. 信息系统

就信息系统而言，我国国家标准 GB/Z20986—2007 信息安全事件分类分级指南中认为，信息系统是“由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统”。从信息的角度来说，我们认为信息系统是为信息生命周期提供服务的各类软硬件资源的总称。

信息系统以信息作为其处理的本质对象，但其作为一种特定的系统，同样具备系统的基本特征。信息系统是信息在生命周期中的生存环境，即：信息是信息系统的处理对象，信息系统是信息赖以生存的环境。

1）有机构成

信息系统通常由计算机软硬件系统、相关物理设备、网络设施等构成。各组成部分相互合作，以完成对信息的采集、加工、存储、传输、检索等处理。

2）整体性和独立性

信息系统的组成部分有机组合构成一个完整的系统，脱离了网络设施将无法实现信息的传输；缺少了计算机软硬件系统将无法对信息进行加工、处理等操作；缺少了相应的设备将无法实现信息的输入、输出。

3）层次性和聚合性

信息系统可作为子系统，从而构成功能更加强大、更复杂的信息系统。而将若干信息子系统构成一个信息系统的过程，我们通常称为集成。这体现了信息系统的聚合性。

4）稳定性

信息系统投入正式运行后，在一段时间内存在功能的稳定性。但由于用户需求的变化以及信息技术的发展，信息系统将面临着不断的升级、更新和发展演化。

5）安全属性

信息是信息系统处理的直接对象。信息的安全属性是通过信息系统来实现和提供的，这涉及信息的可用性、机密性、真实性、完整性、可控性、可靠性、可追溯性等若干安全属性。

1.2 系统集成

在定义和理解了信息系统概念的基础上，我们来进一步了解系统集成的概念。在这个词汇中，“集成”是主体。

1. 集成

集成（Integration）就是一些孤立的事物或元素通过某种方式集中在一起，产生联