信息安全保障人员认证培训教材

信息系统安全运维

XIN XI XI TONG AN QUAN YUN WEI

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 刘 韧 皮志贤 王 惠 马庆余

★★★ CISAW ★★★

电子科技大学出版社

信息安全保障人员认证培训

信息系统安全运维

XIN XI XI TONG AN QUAN YUN WEI

中国信息安全认证中心

主 编 张 剑 ◎副主编 刘 韧 皮志贤 王 慧 马庆余

★★★ CISAW ★★★

电子科技大学出版社

图书在版编目（CIP）数据

信息系统安全运维 / 张剑主编. ——成都 ：电子科技大学出版社，2016. 4

ISBN 978－7－5647－3542－5

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息系统－安全技术 Ⅳ. ①G202

中国版本图书馆 CIP 数据核字（2016）第 072185 号

内 容 提 要

本书在《信息安全技术》阐述的 CISAW 信息安全保障模型基础上，深入诠释了“安全运维”和“运维安全”的核心概念，独具特色地提出信息安全运维业务中“安全运维”和“运维安全”的保障模式，对模型中安全运维活动涉及的运维主体、运维对象、运维流程、运维支撑平台及运维活动等环节进行全面论述，并从风险管理的角度探讨在安全运维过程中如何降低安全风险、保障运维安全。本书结合具体案例阐述模型中涉及的各项活动，重点讲述安全策略、运维准备、运维实施、运维安全、评审及改进活动中的具体工作，为各领域从事信息运维服务人员、系统运维单位管理者和信息运维单位的运维管理者提供信息安全技术支撑。

信息系统安全运维

主 编 张 剑

副主编 刘 韧 皮志贤 王 惠 马庆余

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： 万晓桐 徐守铭

责任编辑： 万晓桐 徐守铭

主 页： www. uestcp. com. cn

电子邮箱： uestcp@uestcp. com. cn

发 行： 新华书店经销

印 刷： 成都市火炬印务有限公司

成品尺寸： 185mm×260mm 印张 17.5 字数 482 千字

版 次： 2016 年 5 月第一版

印 次： 2016 年 5 月第一次印刷

书 号： ISBN 978－7－5647－3542－5

定 价： 60.00 元

本书编委会

副主编： 刘　韧　皮志贤　王　惠　马庆余

编　委： 韩　震　王　旭　时　鹏　周艳芳　李　洁　王　建
梁　浩　龚钢军　范杰清

丛书编委会

主　任： 魏　昊

副主任： 丁元汉　陈晓桦　吴晓龙　亓明和

委　员： **（按姓氏笔画排序）**

丁元汉　丁　峰　于春刚　万里冰　马卫东　马庆余
王　刚　王怀宾　王　莉　王夏莲　王　强　王　静
王　惠　王　旭　王　建　亓明和　尹远飞　尹朝万
邓　刚　甘杰夫　皮志贤　史小卫　冯　丽　冯　峰
成林芳　朱灿庭　朱　强　华颜涛　刘春旺　刘春波
刘　洋（广东）　刘　洋（辽宁）　刘润乾　刘　韧
汤志伟　孙　爽　杜孝伟　李　洁　李　倩　李　源
时　鹏　杨惟泓　肖鸿江　吴永东　吴芳琼　吴晓龙
何一丁　宋　杨　宋明秋　张会平　张良龙　张　剑
张徐亮　张　雪　张维石　张　斌　范杰清　陈　宇
陈晓桦　武　刚　林　利　林海峰　罗小兵　罗俊海
岳笑含　周佩雯　周福才　周艳芳　郑　莹　赵国庆
赵　洋　赵　辉　胡　松　钟　毅　段先斐　段静辉
秦潇潇　钱伟中　徐全生　徐　俊　徐　剑　徐　然
高天鹏　郭心平　郭剑锋　梁　浩　龚钢军　蒋　军
蒋宏伟　韩　征　韩　震　傅　翀　谢　兄　蓝　天
雷　冰　蔡运娟　廖国平　翟亚红　熊万安　潘　伟
魏　昊

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，其中包括《信息安全技术》《信息安全技术应用》和《信息安全实验》等3本基础教材；《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》《电子认证技术》和《工业控制信息安全》等13本专业技术应用教材；《电子政务安全》《电子商务安全》《CA服务安全》《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》等 11 本应用领域教材。

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

《信息系统安全运维》一书基于长期从事信息安全服务和信息系统运维服务的实践，在参考国内外的最佳实践基础上，系统地介绍安全运维的概念，安全运维主体、对象、流程、支撑平台及运维活动的各个环节，着重介绍在安全运维过程中如何减低安全风险、保障运维安全。本书提出了信息系统安全运维模型，该模型是在 CISAW 信息安全保障统一模型的基础上衍生的，模型涵盖了“安全运维”和“运维安全”两种模式，本书以安全运维模型的两种模式为框架展开，结合运维实例形成了完整的安全运维知识体系。

本书共分为 9 章，第 1 章是概述，从信息系统运维的基本定义出发，重点介绍了本书的核心模型——信息系统安全运维模型；第 2 章安全运维知识体系的综述，从安全运维理论的角度介绍安全运维涉及各个环节的基本知识；第 3 章介绍实施安全运维相关法律法规和标准规范；第 4 章至第 6 章分别以案例的方式介绍安全运维活动最重要环节的实施方法，对制定安全策略、实施运维准备以及开展运维活动以明确的工作指导；第 7 章着重介绍安全运维过程中降低安全风险，保障信息系统运行的方法；第 8 章对安全运维过程进行有效性评估，并提出从日常运维和应急体系完善角度提出了持续改进方法；第 9 章为认证培训的学员对相关的服务资质认证标准进行解读，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，同时也合适所有从事与信息系统运维有关的技术人员和管理人员以及期望了解信息安全运维相关知识的人员使用。本书在成书过程中得到了中国信息安全

认证中心、华北电力大学信息安全工程实验室、四川省中认信安技术服务有限公司、北京华电卓越国际技术培训有限责任公司、北京赛虎网络空间安全技术发展有限公司、北京华电卓识信息安全测评技术中心有限公司、北京卓越蓝军信息安全技术发展有限公司的大力支持，在此表示衷心感谢。

本书由张剑、刘韧、皮志贤、王惠、马庆余、韩震、王旭、时鹏、周艳芳、李洁、王建、梁浩、龚钢军、范杰清等共同编写，本书在编写过程中参考或引用了国内外同行的大量资料或观点，在此向这些作者表示衷心感谢。

本书力图以真实的案例、清晰的结构和流畅的语言来展现本书的知识体系、但由于水平有限、时间紧迫、尽管我们进行了多次研讨和修订，书中仍难免存在疏漏和错误。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

2016 年 5 月 16 日

目录
Contents

第1章 概 述

随着信息技术的高速发展和信息化进程的不断加快，人们对信息系统的依赖程度日益增加，信息安全问题受到普遍关注。由于信息系统在开发设计、部署实施及运行维护等阶段对安全性考虑甚少，存在着不完善、不可靠、不稳定的因素，在信息系统运行过程中，信息系统运行失效、系统宕机、信息泄露、内容篡改等安全事件时有发生，保障信息系统安全运行成为系统运维人员必须首要考虑的大事。

在信息安全形势日益严峻的时代，大多数运维服务工作处于一个被动状态，主要表现在：安全设备的种类和数量越来越多，并未发挥应有的安全防护作用；运维人员技术水平参差不齐，在发生安全事件时往往茫然不知所措。

问题集中体现在以下几个方面。

（1）众多安全设备缺乏有效的统一管理；

（2）由于安全配置不当导致衍生安全风险；

（3）安全运维能力不足，5×8 小时外的安全事件无暇顾及；

（4）信息安全产品种类太多、更新太快；

（5）缺乏专业的安全运维团队；

（6）突发安全事件的应急处理能力不足；

（7）异常操作行为无法及时预警；

（8）信息管理部门的人员有限，员工的精力有限；

（9）安全管理制度体系不完善，安全责任制落实不到位；

（10）安全技术能力方面存在不足。

信息系统的稳定运行与信息安全密不可分，运维人员需要管理越来越庞大的 IT 系统，对系统进行定期检查和维护，减少安全事件发生的可能，保障信息系统稳定、高效运行。因此，安全运维不仅仅要保障安全措施足够全面，及时处置各类安全事件，还要保障安全处置不会给在运信息系统带来衍生安全风险。

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。

1.1.1 信息

长期以来，信息的定义一直是科学家讨论的话题。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 GB/T 4894—2009《信息与文献 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的“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信息的产生、存储、传输、处理和销毁等诸多环节。

信息具有以下特性。

1）承载性

信息要表达一定的意思，因此信息承载着意义；信息必须借助文字、图像、声音、光波等物质形式而存在或表现，因此信息必须被载体所承载。能用于记载信息的物质称为信息载体，人的大脑是最复杂的信息载体，各种数据均为信息载体。

2）传输性

信息可以由信息源通过载体传播到接收者。信息在传播过程中，其形式可能会发生变化，但其内容不会改变。信息传播的速度和效率取决于传播载体和传播手段。

3）层次性

信息所反映的意义具有不同的抽象层次。比如企业的信息可分为战略层的信息、策略层的信息和执行层的信息。

4）共享性

一个信息源可以到达多个信息接收者，被多个人所共享。它的共享性使得它获得广泛的应用。

5）加工性

加工是指对信息的整理、变换、压缩、分解、综合、排序等处理。通过对信息进行加工，可以使信息增值。加工的手段决定了人们对信息再利用的水平。

6）时效性

信息的利用往往滞后于信息的产生，但有一定的时限，超过了这个时限，信息就失效。

1.1.2 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/T 20261—2006《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；通过运维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。

《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。

可见系统具有如下几个基本特征。

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个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。

1.1.3 信息系统

就信息系统而言，我国国家标准 CB/Z 20986—2007《信息安全技术 信息安全事件分级指南》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