信息安全保障人员认证考试用书

# 信息安全技术

XIN XI AN QUAN JI SHU

主　编　张　剑

副主编　罗小兵　万里冰


电子科技大学出版社

信息安全保障人员认证考试用书

# 信息安全技术

主　编　张　剑

副主编　罗小兵　万里冰


电子科技大学出版社

**图书在版编目（CIP）数据**

信息安全技术 / 张剑主编. —成都：电子科技大学出版社，2013.12

ISBN 978-7-5647-2163-3

Ⅰ. ①信… Ⅱ. 张… Ⅲ. ①信息安全-安全技术 Ⅳ. ①TP309

中国版本图书馆CIP数据核字（2013）第310684号

## 内 容 提 要

本书从信息安全保障WPDRRC模型出发，从应用的视角诠释了信息安全的基本概念与技术，包括密码编码与密码分析、身份认证与访问控制、网络风险与边界防护、平台风险与安全防护、应用风险与安全开发、数据风险与保护措施、物理风险与安全保障以及IPv6的有关信息安全问题。学习本书能全面地掌握信息安全保障工作所需的基本知识，较好地完成认证考试。

本书是信息安全保障人员认证考试用书之一，既可供信息安全保障人员培训使用，也可供对信息安全技术感兴趣的读者阅读使用。

# 信息安全技术

**主　编**　张　剑

**副主编**　罗小兵　万里冰

**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**：郭蜀燕　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**：成都蜀雅印务有限公司

**成品尺寸**：185 mm × 260 mm　　**印张** 16.75　　**字数** 350千字

**版　　次**：2013年12月第一版

**印　　次**：2013年12月第一次印刷

**书　　号**：ISBN 978-7-5647-2163-3

**定　　价**：42.80元

# 编委会



# 编写组


**主　编**　张　剑

**副主编**　罗小兵　万里冰

**编　委**　王佳昊　钱伟中　秦潇潇　蓝　天

# 前　言

《信息安全技术》是“信息安全保障人员认证（Certified Information Security Assurance Worker，CISAW）”系列考试用书中正式推出的第一本参考用书，是CISAW总结的信息安全知识体系中基础知识部分的核心内容。

职业教育重在技术应用，本书力求从实际应用的需要出发，讨论目前信息安全保障工作中主要应用的专业技术。全书共9章，第1章从信息安全保障基本模型出发，阐述信息安全的基本对象和概念；第2章从密码学的历史出发，阐述密码的基本原理和应用方法；第3章抓住身份认证和访问控制这一核心要素，阐述安全控制的本质及应用方法；第4章从网络防护的实际需求出发，讨论典型的防护手段及其基本原理；第5章在深入分析相关风险的基础上，就操作平台和应用平台的典型防护技术进行了阐述，且讨论了具体的防护措施；第6章面对日益严重的应用安全提出了具体的风险分析方法和提升应用安全保障能力的措施；第7章针对信息系统中的数据安全进行了专门的分析，结合实际数据保护技术讨论了数据保护的具体方案；第8章就典型的物理安全问题进行了总结，且提出了有效的防护措施；第9章为不断提升技术人员跟踪新技术的能力，专门将IPv6的基本概念介绍和IPv6安全作为额外奉献呈现给大家。

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，也适合所有从事与信息技术安全相关的工作人员以及期望了解信息安全技术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和《信息安全保障人员认证考试用书》编委会的大力支持，在此表示衷心感谢。

在编写过程中得到了电子科技大学陈伟、傅翀、王星、屈宏、陈浩等教师和学生的大力帮助，在此表示衷心感谢。

在出版过程中，得到了四川亚和企业咨询管理有限公司的多方支持，在此表示衷心感谢。

本书的编写参考或引用了国内外同行的大量文献资料，在此向这些文献资料的作者表示衷心感谢。

我们力图通过较小的篇幅比较完整地、正确地介绍信息安全相关的基本技术，同时，为了能够扩大读者面，尽量使用简单、实用和易于理解的方式进行阐述。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

2013年11月

# 目　　录

# 第 1 章　信息安全基础

随着计算机及通信技术的广泛应用，信息技术得到了高速发展。信息技术给人们生活带来了新的模式和诸多便利，支撑着政府和社会各行各业日常业务的开展，这对信息安全技术提出了严峻的挑战。近年来，信息安全问题日益突出，如何为信息化的开展提供信息安全保障是国家信息化建设、国家安全的重要课题。

信息安全是一门重要的学科，涉及计算机、通信、数学、密码学等诸多领域，是一个综合性的科学体系。本章通过相关模型向读者介绍信息、信息安全及信息安全保障的基本概念。

## 1.1　WPDRRC 与 PDRR 模型

模型是人们认识和描述客观世界的一种方法。在信息安全的研究和应用中，通常采用的模型有：PDR（防护、检测和响应）、PPDR（策略、防护、检测和响应）、PDRR（防护、检测、响应和恢复）、MPDRR（管理、防护、检测、响应和恢复）和我国的 WPDRRC（预警、防护、检测、响应、恢复和反击）等动态可适应安全模型。

PDR 模型由防护（Protection）、检测（Detection）、响应（Response）三部分组成。PPDR 模型是在 PDR 模型的基础上增加了策略（Policy）组件。根据 PPDR 模型，一个完整的动态安全体系，需要在协调的、一致的安全策略指导下实施恰当的防护、动态的检测，并进行实时响应，形成一个完备的、闭环的动态自适应安全体系。WPDRRC 安全模型是我国 863 计划信息安全专家组在 PDR 模型、P2DR 模型及 PDRR 模型的基础上提出的适合我国国情的网络动态安全模型。

WPDRRC 模型[1]在 PDRR 模型 4 个环节的基础上增加了预警（Warning）和反击（Counterattack）两个组件，共计 6 个环节。它们形成了具有动态反馈关系的整体。预警组件根据已掌握的系统脆弱性以及威胁发展趋势，预测未来可能受到的攻击与危害；反击则是采用一切可能的技术手段，获取有关威胁行为的线索与证据，形成强有力的

取证能力和依法打击手段。WPDRRC 模型增加了人、政策和技术三大要素，其中“人”是内层，是基座与核心；“政策”主要包括法律、法规、制度和管理，是中间层；“技术”是外层，它落实在模型 6 个环节的各个方面，它的操作必须受到人和政策的制约。WPDRRC 模型如图 1 所示。

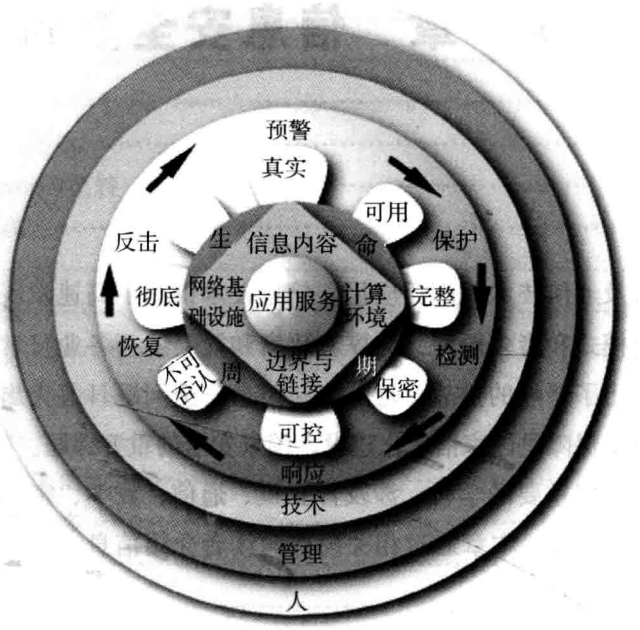


图 1 - 1　WPDRRC 模型

在 WPDRRC 体系模型中，人员在管理和策略的约束和指导下，利用信息安全技术为信息在整个生命周期中提供真实性、可用性、完整性、保密性、可控性、不可否认性等安全特性的保障。该保障过程分为预警、防护、检测、响应、恢复和反击 6 个环节及能力。而信息生命周期中涉及的信息内容、计算环境、网络基础设施、边界与链接等诸多方面，它们均通过平台支撑着信息系统应用程序的运转。

本书以信息安全技术为题，处于该模型的“技术”层，主要介绍信息安全保障的相关技术，以及如何将这些技术应用于 WPDRRC 模型的各个环节，为信息、信息系统提供上述的安全特性。

### 1.1.1　信息定义

1948 年，C. E. Shannon 博士在“通信的数学理论”一文中，从数学的角度给出了信息的定义，他认为：“The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant

to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages.”即“通信的基本问题是再制造一点或者准确地或者近似地一个从别处挑选的信息。通常信息有意义，那是他们提到的或是依照一些特定物质或概念上实体的系统的相互关联。这些与语意有关的通信方面是不切题的工程问题。重要的方面是真实的信息是从一组可能的信息挑选来的。”

我们认为信息是一种实体对象，能够通过信息系统进行处理。信息通过载体在一定环境中表现、存储和传输。信息作为实体对象，和自然界其他对象一样，有产生、发展和消亡的过程，我们称之为生命周期。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。信息系统正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，信息系统是信息的生存环境。

我国国家标准（简称国标）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。

### 1.1.2　安全定义

简单地说，所谓安全就是“不出事或感觉不到要出事的威胁”。可见，安全关乎两件事：一件是已经发生的事，即安全事件；另一件是未发生但可能引发安全事件的事，即安全威胁与脆弱性。例如：操作系统遭受漏洞型病毒攻击事件属于已经发生的安全事件；而操作系统没有更新补丁而存在被攻击的系统漏洞则是属于系统的脆弱性，是可能导致发生安全事件的事。

根据上述观点，要解决安全问题必须从这两个方面入手，做好安全事件的处理和应对，同时做好安全威胁的防范和脆弱性的避免。就信息安全问题而言，这两个方面的工作分别对应着 WPDRRC 模型的响应与恢复环节、防护与检测环节。

信息的安全问题是本书讨论的核心问题。信息安全可被理解为信息系统抵御意外事件或恶意行为的能力，这些意外或恶意事件和行为将破坏由信息系统所提供的可用性、机密性、完整性、不可否认性、真实性等安全特性[2]。这些安全特性是信息安全的基本属性。

### 1.1.3　可用性

可用性，在国家标准 GB/T9387.2－1995 和公安部标准 GA/T 391－2002 中，被定义为“根据授权实体的请求可被访问与使用”。

在 ISO 13335－1：2004 标准中，可用性定义为：“已授权实体一旦需要就可访问和使用的特性”。

在 ISO 17799 - 2000 标准中，可用性定义为："确保已授权用户在需要时可以访问信息和相关资产"。

GASSP（Generally Accepted System Security Principles）认为："可用性是数据的一种特征，指的是在合适的时间，以要求的方式，信息与信息系统可以被访问与可以使用"。

International telecommunication union document CNI/03 中指出，可用性指"使网络在极端环境下运行，也能够在任何时间访问网络上的数据"。

《美国法典》第 44 编第 3542 节中指出，可用性指"确保及时和可靠地访问和使用信息"。

在 NIST SP 800 - 37 2002 V. 1 中指出，可用性是"确保授权用户和/或系统过程可以及时可靠地访问信息\服务和 IT 资源，并能防止拒绝服务（DoS）"。

可用性要求包括信息、信息系统和系统服务都可以被授权实体在适合的时间，以要求的方式，及时、可靠地访问，甚至是在信息系统部分受损或需要降级使用时，仍能为授权用户提供有效服务。

需要指出的是，可用性针对不同级别的用户提供相应级别的服务。对于信息访问的具体级别及形式，由信息系统依据系统安全策略，通过访问控制机制执行。

此外，我们认为信息的可用性与硬件可用性、软件可用性、人员可用性、环境可用性等方面有关。离开信息环境空谈信息的可用性也是不科学的。

### 1.1.4 完整性

国军标 GJB 2256 - 94 中指出：完整性是"信息系统中的数据与在原文档中的相同，并未遭受偶然或恶意的修改或破坏时所具有的性质"。

国标 GB/T 9387.2 - 1995（ISO 7498 - 2 - 1989）中定义：完整性是"这一性质表明数据没有遭受以非授权方式所作的篡改或破坏"。

国标 GB 15852 - 1995（ISO/IEC 9797：1994），GB/T 9387.2 - 1995，GB/T 17903.1 - 1999 等中指出，完整性是"指数据没有被非授权地改变或破坏的性质"。

美国 NIST SP 800 - 37 2002 V1 中定义完整性为："保证对 IT 系统中的信息进行保护，使其不会遭到未经授权的、非预期的或无意的修改或破坏。系统完整性还表达了 IT 系统的质量，它反映了操作系统的逻辑正确性和可靠性，实现保护机制的硬件和软件的逻辑完备性、数据结构和存储数据实例的一致性"。

CNSS Instruction No. 4009 NATIONAL INFORMATION ASSURANCE（IA）GLOSSARY Revised May 2003（国家信息保障词典）中指出："一个信息系统反映逻辑正确性和其操作系统可靠性、硬件和软件执行其保护机制的逻辑完备性、数据结构的一致性、存储数据事故的属性。注意，在一个形式化的安全模型中，完整性狭义地被解释为保护和防止对信息的未经授权的修改或破坏"。

从单纯考虑数据的完整性，发展到兼顾操作系统的逻辑正确性和可靠性，到实现保护机制的硬件和软件的逻辑完备性、数据结构和存储实例的一致性，NIST 的这些说法来源于大量的事实。目前发现：系统中存在的大量漏洞（脆弱性）从根本上说就是因为逻辑的正确性和可靠性出现问题所致，尤其是在信息系统的核心——操作系统中影响最为严重，这个问题当然也存在于实现保护机制的软件、硬件中。这个问题的提出，指出了一个明确的但难度极高的奋斗目标——正确地实现逻辑，同时也指出了完整性的破坏来自三个方面的因素：未授权、非预期、无意。信息技术发展迅速，在技术的应用过程中，除了人为恶意的破坏外，还存在由于能力素质达不到要求可能出现的误操作，和没有预期的系统程序漏洞造成的误动作。它们同样影响完整性，同样需要采取完整性保护措施来加以防范。

### 1.1.5　机密性

国军标 GJB 2256－94 中指出：机密性是“为秘密数据提供保护状态及保护等级的一种特性”。

美国 NIST 特别出版物 800－26《IT 系统安全自评估指南》中提到，机密性是“信息要求得到保护，以免被非授权泄露”。

ITSEC 把机密性定义为：“防止信息的非授权的公开”。

ISO 17799－2000 中指出，机密性为：“确保信息仅被已授权访问的人访问”。

ISO/IEC 的相关标准中，定义机密性为：“信息不能被未授权的个人、实体或者过程利用或知悉的特性”。这些标准包括：ISO/IEC 13335－1：2004－11－15 WG1，ISO/IEC FCD 24743：2004－11－25 WG1，ISO/IEC FDIS 18033－4：2004－12－17 WG2 和 ISO/IEC 21827：2002－10－01 WG3。

这些定义的演变意味着人们认识的深化。从机密性定义的变化可以看出，我们首先认识的是信息不要泄露，因而要对其实施保护。逐渐认识到其中涉及授权问题，即信息的泄露就是对非授权者的公开。继而又意识到从正面看保密性要求，是仅被授权者访问的问题。

此外，大家都知道，机密性要求存在等级的不同。不同机密性等级的信息访问由信息系统的访问控制部件依据系统安全策略及访问控制模型执行控制。

随着信息技术的发展，信息系统的组成是人和机器的结合体，其实体对象不仅包括用户，同时也涉及代表或被用户使用的自动化机器和软件逻辑实施的过程。这些实体，同样需要依据机密性等级进行访问控制。

### 1.1.6　真实性

在 NIST SP 800－37 2004 版本中，明确定义真实性是“能够核实和信赖一个合法的传输、消息或消息源的真实性的性质，以建立对其的信心”。

ISO/IEC 的相关标准（ISO/IEC 13335 - 1：2004 - 11 - 15 WG1，ISO/IEC 21827：2002 - 10 - 01 WG3）中指出，真实性是“保证主体或资源确系其所声称的身份的特性。真实性应用于诸如用户、过程、系统和信息等的实体”。

真实性包含了对传输、消息和消息源的真实性进行核实，它的内涵要求不能被完整性所代替。它不仅是对技术保证的要求，也是对人员责任的要求。

真实性要求对用户身份进行鉴别，对信息的来源进行验证。而这些功能都离不开密码学的支持。在非对称密码机制出现以前，这是一个很大的难题。非对称密码机制的出现，使该项难题得到了解决。随着人类社会步入信息时代，信息的真实性安全属性更加得到人们的重视。

### 1.1.7 不可否认性

在 NIST SP 800 - 37 2004 版本中指出，不可否认性是保证信息的发送者提供的交付证据和接受者提供的发送者证据一致，使其以后不能否认信息传输过程。

国际标准 ISO/IEC 13335 - 1：2004 - 11 - 15 WG1 中认为，不可否认性是“证明一个行为或者事件已经发生的能力，以致事后不能否认这个事件或者行为的发生”。

不可否认性也称为抗抵赖或不可抵赖性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。发送方不能否认已发送的信息，接收方也不能否认已收到的信息。

ISO 7498 - 2 中给出了抗抵赖（non - repudiation）的定义：抗抵赖用于对网络的交互动作进行事后的责任追查和审计，具体可以有原发抗抵赖（防止发送者否认）和带交付证实的抗抵赖（防止接收者否认）[4]。

在当今各类业务信息系统迅猛发展的信息时代，信息不可否认性的安全属性是诸如电子商务等基于信息系统的各类业务得以正常开展的保障。

### 1.1.8 其他属性

除可用性、完整性、机密性、真实性和不可否认性以外，受到研究者关注的还有信息的可靠性和可控性。

可靠性是指与预想的行为和结果相一致的特性。

可控性是指对信息的传播及内容具有控制能力的特性，授权机构可以随时控制信息的机密性，能够对信息实施安全监控。

## 1.2 信息安全保障对象

信息安全保障的直接对象是信息，利用针对信息、载体及信息环境的相关安全技术，实现对信息安全的保障，而信息安全保障的最终目的则是提供组织业务的连续性。

信息安全保障利用与信息、载体和环境相关的安全技术来保障信息的安全。这些技术包括密码学及应用技术、网络安全技术、平台安全技术、应用安全技术、数据安