信息安全保障人员认证培训教材

信息安全风险管理

XINXI ANQUAN FENGXIAN GUANLI

（修订版）

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 廖国平 汤 亮

★★★ CISAW ★★★

电子科技大学出版社

信息安全保障人员认证培训教材

信息安全风险管理

XINXI ANQUAN FENGXIAN GUANLI

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 廖国平 汤 亮

★★★ CISAW ★★★

（修订版）

电子科技大学出版社

图书在版编目（CIP）数据

信息安全风险管理 / 张剑主编. —修订版. —成都：电子科技大学出版社，2016.12

ISBN 978-7-5647-4105-1

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息安全－风险管理 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2016）第 321035 号

内 容 提 要

本书从信息安全风险管理模型出发，以信息安全风险管理为重点，全面介绍信息安全风险管理的基本概念、信息安全风险管理相关国际以及国家标准、信息安全风险评估技术、信息安全风险处置以及信息安全风险管理实例。

本书以信息安全风险管理为主线，内容结构合理，层次分明，重点明确，注重信息安全风险管理实践应用。

本书是信息安全保障人员认证考试用书之一，既能供信息安全保障人员培训使用，也可供对信息安全风险管理感兴趣的阅读者使用。

信息安全风险管理（修订版）

主　编　张　剑

副主编　廖国平　汤　亮

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 9.5　字数 240 千字

版　　次：2016 年 12 月第二版

印　　次：2016 年 12 月第一次印刷

书　　号：ISBN 978-7-5647-4105-1

定　　价：60.00 元

丛书编委会

编 写 组

主　　编：张　剑

副 主 编：廖国平　汤　亮

编著人员：成林芳　王　刚　李　源

吴芳琼　尹远飞　雷　冰

段先斐　朱灿庭

编委人员：潘　伟　林　利　邓　燕

徐　俊　陈　琛

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，截止到 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》3 等本基础教材；《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

《信息安全风险管理》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一本风险管理参考用书，是CISAW的信息安全知识体系中风险管理的核心内容。

本书力求从实践需要出发，讨论当前信息安全保障工作中的风险管理技术。全书共分为5章，第1章从信息安全风险管理基本模型出发，阐述风险的起源、特性、要素及其关系和风险管理的基本概念；第2章从信息安全风险管理标准出发，阐述ISO/IEC31000、ISO/IEC13335、ISO/IEC27005、卡内基梅隆OCTAVE、GB/T20984等相关标准的内容；第3章关注的是风险管理中的风险评估这一核心要素，详细阐述了信息安全风险评估内容，主要按照风险识别、风险分析、风险评价这样一条主线展开论述，同时辅以部分实例进行说明；第4章从风险处置的角度出发，详细阐述风险处置的过程框架，并讨论了几种典型的风险处置措施及其应用；第5章则是从整体的角度出发，依照本书中第1章提出的风险管理基本模型，以一个实际项目作为案例，对整个风险管理的实施过程进行论述。

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，也适合所有从事信息安全风险管理相关工作的人员以及期望了解信息安全风险管理相关知识的人员使用。

本书在编写过程中，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，在此表示衷心的感谢。

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。

编　者

目 录

第1章　概　述

1.1　风险起源

1.1.1　风险概念的由来

“风险”一词由来已久，最普通的说法是：以打鱼捕捞为生的渔民们，每次出海前都要祈祷，祈求神灵保佑自己能够平安归来，其中祈求的主要内容就是让神灵保佑自己在出海时能够风平浪静、满载而归；他们在长期的捕捞实践中，深深地体会到“风”给他们带来的无法预测、无法确定的危险，他们认识到，在出海捕捞打鱼的过程中，“风”即意味着“险”，“风险”一词也因此而得来。

另一种经由多个研究者论证的“源出说”称，风险（risk）一词是舶来品，一部分人认为其来源于阿拉伯语，也有一部分人认为其来自于西班牙语或者是拉丁语，但公认度较高的一种说法是“风险”一词来源于意大利语的“RISQUE”。在最初的运用中，风险也是被理解为客观存在的危险，例如在航海过程中遇到的礁石、风暴等事件或者其他一些非正常的自然现象。

人们对于风险的理解和定义是随着人类文明的进步而不断发展和变化的。大约到了19世纪，经过两个多世纪的发展，风险的概念与人类的决策和行为后果有了更为紧密的联系，并且逐渐被视为影响个人和群体事件的特定方式。“风险”一词的使用，也从早期的航海贸易行业和保险业渐渐衍生到其他行业之中。

现代意义上的风险，已经大大超越了“遇到危险”的狭义含义，而是“遇到破坏或损失的机会或危险”。到了近现代社会，风险一词越来越被概念化，并随着人类活动的复杂性和深刻性而逐步深化，且被赋予了更广泛更深层次的含义。从风险的概念出现到目前，人们对于风险的理解一直在不断地发展和演进中：1987年，Wison在*SCIENCE*杂志上发表了风险相关的文章，并将风险的本质阐述为“不确定性，定义为期望值”；1989年，Maskrey定义风险是“某种自然灾害发生的可能性”；1991年，联合国赈灾组织定义“风险是在特定的区域以及给定的时间段内，由某种自然灾害而导致的人们生命财产和经济活动的期望损失值”；1997年，Tobin和Montz定义“风险是某一个灾害发生的可能性概率和期望损失的乘积”；1998年，Deyle定义“风险是对某一灾害概率与结果的描述”；2007年6月，ISO（国际标准化组织）技术管理局将风险定义为“对目标的不确定性影响（effect of uncertainty on objectives）”。

1.1.2　风险定义

ISO/IEC 31000将风险的定义为：“对目标的不确定性影响。”

从 ISO 技术管理局对风险的定义可以看出，风险是一种影响，影响可能是正面的，也可能是反面的。正面的影响会给我们带来机会与利益，相反就会给我们带来威胁与损失。就像我们平常坐飞机存在失事的风险，正常情况下，飞机可以让我们到达目的地的旅途时间大为缩短，然而，一旦飞机失事，我们付出的可能就是生命的代价。风险被人们大致划分成三个类型：

- 危险因素（或者纯粹的风险），如盗窃等；
- 控制性风险（或者不确定性风险）；
- 机会（投机性）风险，如企业的投资行为等。

风险是针对某个目标而言的，离开了目标而谈论风险是没有任何意义的。目标是组织的目标或者利益相关方的目标，并且它是具体的，而不是抽象的。

风险往往具有潜在事件与后果，或者潜在事件与后果两者相结合的特征。从这一点我们可以看出，事件是风险的一个载体。如果没有安全威胁事件，就谈不上安全威胁事件的可能性及其影响，而没有了可能性与影响，风险也就无从谈起。所以，在我们的风险评估实践中，风险是由可能性与后果的组合来计算的。

当然，能够影响目标的因素有很多种，风险所涉及的只是其中的一种因素，那就是“不确定性”。从 ISO 对风险的定义我们可以看得出来，“不确定性”是风险最本质的特征，它指的是缺乏或者部分缺乏对某个事件及其后果或者该事件发生的可能性的相关信息的了解或者认识的状态。不确定性包含事件发生与否的不确定、发生时间的不确定与影响结果的不确定。

本书重点关注的内容是信息安全风险，对于信息安全风险，本书的定义为“威胁利用脆弱性对风险管理对象所造成的不确定性影响”。

这个概念跳出了传统的“为了安全信息而信息安全”的理解，它强调的是基于业务风险方法来组织信息安全活动，其本身只是整个管理体系的一部分。这就要求我们站在全局的观点来看待信息安全问题。

1.1.3 风险管理的历史

根据维基百科定义，风险管理（Risk Management）是一个管理过程，包括对风险的定义、测量、评估和应对风险的策略。风险管理的目的是将能够避免的风险、成本以及损失最小化。

实际上，风险管理的思想可以追溯到远古时期。面对自然灾害、疾病和外部侵扰，史前人类结为部落，互助互济，共同承担责任，并对各种风险提供保障的方式，这其中渗透着最朴素的风险管理意识和简单的风险管理实践。与风险抗争的长期实践，使人们明白了居安思危、防患于未然的道理，由此产生了早期风险意识和风险管理行为的萌芽。例如，古代中国、古巴比伦、古埃及、古希腊和古罗马等文明古国，很早就有互助共济、损失分摊的风险处理方法，并逐渐演变成现代保险。

自 20 世纪 30 年代风险管理的思想理论开始萌芽后，风险管理逐渐以学科的形式发展起来，并形成了独立的理论体系。此时，风险管理主要运用于企业管理领域，主要目的是对企业的人员、财产和自然、财务资源进行适当保护，风险管理以保险为核心。1950

年，美国学者格拉尔（Russell B.Gallagher）首次使用“风险管理”一词，风险管理的概念开始广为传播。风险管理逐渐成为企业管理领域的一门独立学科。与此同时，有关风险管理的教育和培训的陆续展开以及风险管理咨询公司的出现，推动了风险管理的普及。同时，美国许多大学的工商管理学院和保险系都普遍讲授风险管理课程，将风险管理的教育和培训贯穿于经济管理课程中，许多大学将传统的保险系更名为风险管理与保险系，有关的保险团体也纷纷改名。业界也开始广泛用“风险经理”的职衔来代替“保险经理”的职衔。

20 世纪 70 年代后，风险管理在欧洲、亚洲、拉丁美洲等一些国家和地区获得了广泛的传播，被公认为企业管理领域内的一项重要内容，控制企业环境中的风险和不确定性已成为企业管理的核心问题。同时，风险管理逐步规范化、标准化和程序化，管理方法不断丰富，管理领域不断扩大，逐渐扩大到了社会管理领域，成为政府管理和制定政策的重要方面，科学家成为风险管理的主角。

在 20 世纪 70 年代以前，风险管理主要研究工矿企业的生产安全、投资风险、保险等风险以及地震、海啸、暴风雨、洪水、火灾等自然风险，并涉及核电站设计安全、飞机设计安全等重大工程项目的可靠性和相关风险问题。自 20 世纪 70 年代开始，由于技术进步和技术应用的不确定性，环境、公共安全和健康问题引起了社会公众的关注，学术界开始从环境和社会结构的角度来研究技术风险、健康风险等，并逐步扩大到社会风险等其他领域。随着人口、资源与环境之间矛盾的加大，除了深化技术风险的研究外，人们开始研究涉及人类生存的重大风险问题，如贫困、全球气候变化、能源短缺、核技术和生物技术的控制、全球化、自然灾害中的生命线安全、环境污染、转基因食品安全、禁止克隆人类等热点和焦点问题。在风险管理的应用范围上，由于风险管理中损失控制技术具有极强的普遍性，所以国外企业界、金融界以及政界和军界都在应用风险管理的知识来进行风险规避。特别是在核能管制、环境、能源、公众健康等公共政策制定过程中，公共部门决策者也开始探索使用风险分析的理论与方法。

随着人们对风险的复杂性、多样性、交叉性和不确定性有了进一步的了解，人们从各种技术风险问题中抽象出一些共性的东西。在风险管理方面，人们不仅研究风险事件发生概率的组合，而且更加深入地研究各种风险值模型，计算复杂性系统中各种风险事件出现的可能性。与此同时，在风险管理的技术上，随着计算机和高灵敏度测量仪器功能的不断增强，越来越多的研究者根据实际问题的环境条件建立数学模型进行模拟试验，进行风险分析。

从研究内容来看，理论界开始把风险管理看作是自然科学、社会科学交叉的综合领域。自然科学家们坚持风险客观说理论，试图寻找量化、度量、具体化、计算、科学化、明确风险的途径，他们认为风险可以而且应该被精确和准确地量化。1983 年，美国科学院公布了风险评价的四段法：危险识别、暴露评估、剂量-反应评估、风险描述。1983 年，风险与保险管理协会（RIMS）通过了“101 条风险管理准则”，作为各国风险管理的一般原则，成为风险管理科学化、规范化的标志。从澳大利亚 / 新西兰风险管理标准（Risk Management，AS/NZS4360）的实施开始，一些发达国家纷纷效仿，制定全国性风险管理标准，指导和推动风险管理的发展。相反，社会学家们则提出风险主观说的理论，

将风险当作有机的文化结构，认为对风险的测量、理解和管理行为同时也改变了风险本身。管理风险不应只注重技术与财务，还应该注重个人行为与文化社会背景的影响。为此，英国学者道格拉斯（Mary Douglas）和拉什（Scott Lash）提出了风险文化理论，强调根据不同的价值观和信念可以把人们划分成若干文化群体；吉登斯（Anthony Giddens）提出了“失控的世界”和“人造风险”的观点；德国学者贝克（Ulrich Beck）提出了风险社会理论。这些学者从社会科学的角度来研究风险，强调要将公众的风险观点引入到政策实施中来，理解和接纳公众的风险意识作为有效的风险管理策略的基础，而且还研究风险意识与性别、种族、政治观点、从属关系、情感以及信任程度等的关系。这些风险主观说的理论对风险管理的传统思维冲击很大。

20 世纪 70 年代中期之后，风险管理的概念、原理和实践已从美国传播到加拿大和欧洲、亚洲、拉丁美洲的一些国家，美、英、日、法、德等国纷纷建立全国性和地区性风险管理协会。2001 年“9 • 11”事件后，风险管理进入了一个新的阶段，开始得到各国政府普遍重视，并获得了全方位的发展。各国纷纷投入大量的人力、物力和财力，强调政、研、企多方合作，开展风险管理的理论研究和实际运作。各种国家层面的综合风险管理机构以及跨国、国际性综合风险管理机构纷纷成立。综合风险管理机构最具代表性的是国际风险治理理事会（International Risk Governance Council，IRGC）和“欧洲诚信网络”（Trust net）。2003 年，由有影响力的政府官员、科学家和其他领域专业人士组成了国际风险治理理事会（IRGC），将风险管理从民间学术交流和企业自发推动的层次上升到政府行为层次，标志着政府将在关系国计民生的风险评价和风险管理中发挥更大作用。此外，在国家层面上，许多国家开始建立自己的综合风险管理机构。例如，2001 年，韩国成立了综合性风险管理学会——韩国风险治理学会（Korean Society for Risk Governance，KSRG），该学会由全职相关领域专家组成，包括自然灾害、意外事故、核能、环境、气候、信息系统、公共卫生和健康、生物工程（转基因食品）、食品安全、药物、纳米材料、年龄老化、犯罪、风险心理学和认知学等社会科学和自然科学领域的专家。

从发展趋势来看，风险管理已成为多学科交叉的前沿管理领域，综合了自然科学与社会科学、工程技术与管理科学等多学科和多领域。

理想中的风险管理在事先就已经排定好优先次序，对于引发最大损失以及发生概率最高的事件可以优先处理，然后再对风险相对比较低的事件进行处理。实际情况中，由于风险与发生概率往往不一致，很难对处理顺序进行事先排序，因此需要衡量两者的比重，从而做出最合适的判断。

1.2 信息安全风险管理

伴随着信息技术的飞速发展和社会信息化进程的不断加快，国民经济乃至国家安全对信息和信息系统的依赖程度越来越大。因此，信息的安全性已经引起了国家的高度重视。信息安全管理是对一个组织或机构中信息系统的生命周期全过程实施符合安全等级责任要求的科学管理，它包括：落实安全组织及安全管理人员，明确角色与职责，制订

安全规划；开发安全策略；实施风险管理；制订业务持续性计划和灾难恢复计划；选择与实施安全措施；保证配置、变更的正确与安全；进行安全审计；保证维护支持；进行监控、检查，处理安全事件；安全意识与安全教育；人员安全管理等。

信息安全管理的本质是风险管理，安全与风险是密不可分的，没有绝对的安全也没有彻底的风险。信息安全风险管理是一个持续的管理过程，整个过程包含建立合适的风险管理框架、实施风险评估、利用风险处置计划来实施风险建议和决策并处置风险，最后通过对整个管理过程实施评审以达到整个管理过程的持续改进。信息安全风险管理过程适用于整个组织或者其中的任何部分（如部门、物理区域甚至是一个服务），它也适用于任何的信息系统。

企业的信息安全风险管理应该成为企业管理的组成部分，首先应该制定信息安全管理的策略方针，在此基础上选择控制目标和控制方式，还需考虑控制成本与风险平衡的原则，将风险降低到组织可以接受的水平，整个管理过程需要全员参与，实施动态管理。信息安全管理具有风险管理的基本特征，是遵循 PDCA 环的持续性过程。

有效的风险管理是建立在一定的模型之上的。模型是人们认识和描述客观世界的一种方法。在信息安全保障阶段，通常的模型有：PDR（保护、检测和响应）、PPDR（安全策略、保护、检测和响应）、PDRR（保护、检测、响应和恢复）、MPDRR（管理、保护、检测、响应和恢复）和 WPDRRC（预警、保护、检测、响应、恢复、反击）等动态安全模型。

WPDRRC 安全模型是我国 863 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。预警环节根据已掌握的系统脆弱性以及威胁发展趋势，去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。在 WPDRRC 安全模型的基础上，结合实际应用与认证体系，提出了 CISAW 信息安全保障模型，通过把 CISAW 信息安全保障模型应用到信息安全风险管理领域，得出了一个实际可行的信息安全风险管理模型，如图 1-1 所示。

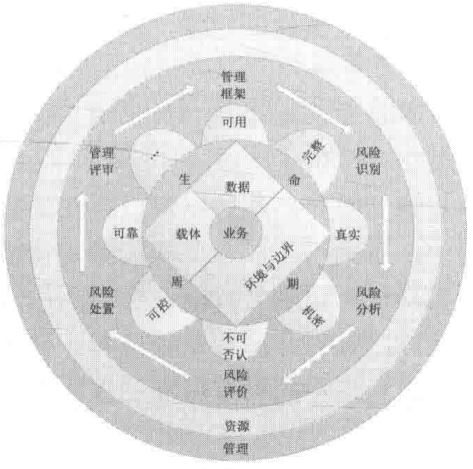

图 1-1　信息安全风险管理模型

1.2.1 信息安全风险管理对象

图 1-1 所示的信息安全风险管理模型中，从核心管理对象——“业务”出发，具体解决数据、载体、环境与边界四个对象全生命周期的信息安全风险管理问题，提供可用性、完整性、真实性、机密性、不可否认性（抗抵赖性）等若干安全属性，并综合协调管理人、技术、财务、信息四类主要资源，在管理框架、风险识别、风险分析、风险评价、风险处置和管理评审的六个环节上实现信息安全风险的管理与监视评审。

1. 本质对象

信息安全风险管理的本质对象是“业务”，“业务”是一个组织的正常运转的核心活动。业务的连续性直接关系到组织是否能够正常履行其职能。组织业务的保障需要组织投入人力、物力和财力资源，维持组织业务的开展。随着信息化水平的提高，业务信息资源的依赖性愈来愈大。与此同时，信息资源所面临的威胁也是越来越多，针对信息资源的攻击手段也越来越多样化。因此，信息资源受到了来自各个方面（主要包括技术与管理两个方面）的风险的威胁。从而使得信息安全风险管理成为信息化组织所必不可少的环节。

例如，某游戏网站业务完全依赖于实时在线的众多游戏玩家，如果该游戏网站遭遇到 DDoS（Distributed Denial of Service）攻击，将使众多玩家无法正常进入网站进行游戏，这会使得玩家对该网站失去兴趣。然而，由于该游戏网站在建设初期就已经意识到网站可能面临被 DDoS 攻击的风险，已经在系统中部署了防 DDoS 攻击的硬件设备，从而使网站从未被可能的 DDoS 攻击所影响。这个例子就很好地体现了风险管理的价值所在。

2. 实体对象

信息安全风险管理涉及四类实体对象，分别是数据、载体、环境和边界。载体在一定的环境中承载信息，并在边界中得到控制。

（1）数据。数据作为实体对象的一种，它通过载体以某种具体的形式来承载。这些形式在信息系统中可以具体到某种数字格式，如视频、声音、图形等，继而具体到数据的具体存储格式，即二进制字节、数据位。这样，保证了具体数据的安全也就确保了其所承载的信息的安全。

（2）载体。由于数据本身不是有形实体，它只是消息、情报、指令和信号中所包含的内容，所以必须利用某种媒介进行存储和传递。

载体是一种数据存储和传输的媒介，是数据赖以存在的物质基础。它是用于记录、传输、汇集和存储数据的实体，包括：①以介质和能源为特征，综合运用电波、光波等传输数据的无形载体；②以实物形态记录为特征，综合运用纸张、胶片、磁盘等存储介质来传递和贮存数据的有形载体。各种介质都是载体的一种形式。信息系统采用物理安全技术以确保介质的物理形式的安全，利用数据安全技术确保数据在介质内逻辑形式的安全。

从某种角度来说，保护载体就是保护数据本身。数据与载体的关系和灵魂与肉体的

关系极为相似，载体的损毁将直接导致数据的消失。

（3）环境与边界。这里的环境指数据与载体的环境，即数据及承载数据的载体在整个生命周期中所依赖的软硬件资源，进而扩展到软硬件资源所处的物理环境等更大的范畴。

在信息环境中，数据在存储介质中存放、在应用信息系统中处理、在网络通信系统中传输。

在物理环境中，一方面需要保障数据载体的物理安全，另外一方面需要保障信息系统及网络系统硬件平台的安全。

1.2.2 信息安全属性

我们认为信息安全是信息系统抵御意外事件或恶意行为的能力，这些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、真实性等基本安全特性。下面将分别对这些基本安全属性进行说明。

1. 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：“可用性是数据的一个特征，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 篇第 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，可用性指“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，并能防止拒绝服务攻击（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、要求的方式、及时可靠地被访问，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。具体对于信息访问的级别及形式，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。

2. 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