注册信息安全专业人员
资质认证培训教材

信息安全标准与法律法规

中国信息安全产品测评认证中心 编著

- 由信息安全专家精心编写与认真审校
- 全面覆盖了信息安全学科的知识要点
- 信息安全人员资质权威认证专业教材

人民邮电出版社
POSTS & TELECOM PRESS

注册信息安全专业人员
资质认证培训教材

信息安全标准与法律法规

中国信息安全产品测评认证中心 编著

人民

图书在版编目（CIP）数据

信息安全标准与法律法规 / 中国信息安全产品测评认证中心编著. —北京：人民邮电出版社，2003.9
注册信息安全专业人员资质认证培训教材
ISBN 7-115-10943-5

Ⅰ. 信… Ⅱ. 中… Ⅲ. ①信息系统—安全技术—标准—世界—技术培训—教材②信息系统—安全管理—法规—世界—技术培训—教材 Ⅳ. ①TP309-65②D912.1

中国版本图书馆 CIP 数据核字（2003）第 078828 号

注册信息安全专业人员资质认证培训教材
信息安全标准与法律法规

◆ 编　　著　中国信息安全产品测评认证中心
责任编辑　杨　璐

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www. ptpress.com.cn
读者热线　010-67132692
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：18.75
字数：448 千字　　2003 年 9 月第 1 版
印数：1-4 000 册　　2003 年 9 月北京第 1 次印刷

ISBN 7-115-10943-5/TP・3262

定价：32.00 元

本书如有印装质量问题，请与本社联系　电话：（010）67129223

内容提要

本书主要针对“注册信息安全专业人员”培训，以注册信息安全专业人员所应具备的知识体系为大纲进行编写。全书主要介绍了包括基础信息安全标准、环境与平台安全标准、信息安全产品标准、信息安全管理标准、信息安全测评认证标准等在内的国内外与信息安全有关的标准，同时，还简述了目前各国信息安全法律法规的发展状况并详细列出了我国现有的信息安全法律法规。通过对本书的学习，信息安全及相关行业的从业人员可对标准的概念、国内外信息安全标准及法律法规有一个较为全面的了解。

本书适合作为信息安全专业人员培训班的培训教材，也可供从事相关工作的技术人员和对信息安全感兴趣的读者阅读参考。

注册信息安全专业人员资质认证培训教材

编委会

丛书序

随着我国社会信息化进程发展，计算机网络及信息系统在政府机构、企事业单位及社会团体的运作中发挥着越来越重要的作用。信息化水平的提高在带来巨大发展机遇的同时也带来了严峻的挑战。由于信息系统本身的脆弱性和日益呈现出的复杂性，信息安全问题不断暴露。信息安全既关系着个人的隐私，也关系着国计民生，乃至整个国家的安全与利益。信息安全问题已经倍受政府和社会的广泛关注和重视。在这样的大背景下，社会对信息安全专业人员的需求逐年增加。据统计，国内从事信息安全方面的专业人员仅有 3000 余人，社会需求与人才供给间还存在着很大差距；怎样培养信息安全的专门人才，并确保现有信息安全从业人员的职业素质等，将成为信息安全产业发展中需要迫切解决的重要问题。

人员认证概述

中国信息安全产品测评认证中心是经中央批准成立，代表国家开展信息安全测评认证的职能机构，“中华人民共和国国家信息安全认证”是目前国家对信息安全技术、产品、信息系统安全质量以及信息安全服务资质、人员资质的最高认可，由中国信息安全产品测评认证中心及其授权测评机构进行评估，由中国信息安全产品测评认证中心进行认证。本丛书是针对“注册信息安全专业人员认证”部分的培训教材。

“注册信息安全专业人员”（Certified Information Security Professional，简称 CISP）是指机构组织中负责信息系统（网络）建设、运行和应用管理的必备的专业性人才，其基本职能是为信息系统的安全提供技术和管理保障。对信息安全专业人员的认证和注册，是提高信息安全从业人员职业道德和技术水平、提升信息安全产业的竞争能力和强化国家信息安全管理的有效手段。

从书内容特色

本套丛书充分考虑“注册信息安全专业人员”培训学习的需要，以注册信息安全专业人员所应具备的知识体系为大纲，从信息安全的理论基础出发，兼顾理论学习与实践应用，较好地反映了信息安全学科的主要内容和基本特点，较为全面地覆盖了学科的知识要点。

为了使广大信息安全技术人员对信息安全有比较系统和全面的了解，本套丛书共分为以下 3 册：

《信息安全理论与技术》

《信息安全工程与管理》

《信息安全标准与法律法规》

内容涉及安全体系、密码技术、网络安全、系统安全、风险评估、安全策略、安全工程、信息安全管理、应急响应、国内外相关标准及法律等诸多方面，使相关从业人员对信息安全学科有一个较为全面的了解。

适用对象

本丛书适合作为培养信息安全专业人员的培训班教材，也适合从事信息安全工作的技术人员和广大对信息安全感兴趣的读者阅读参考。

关于作者

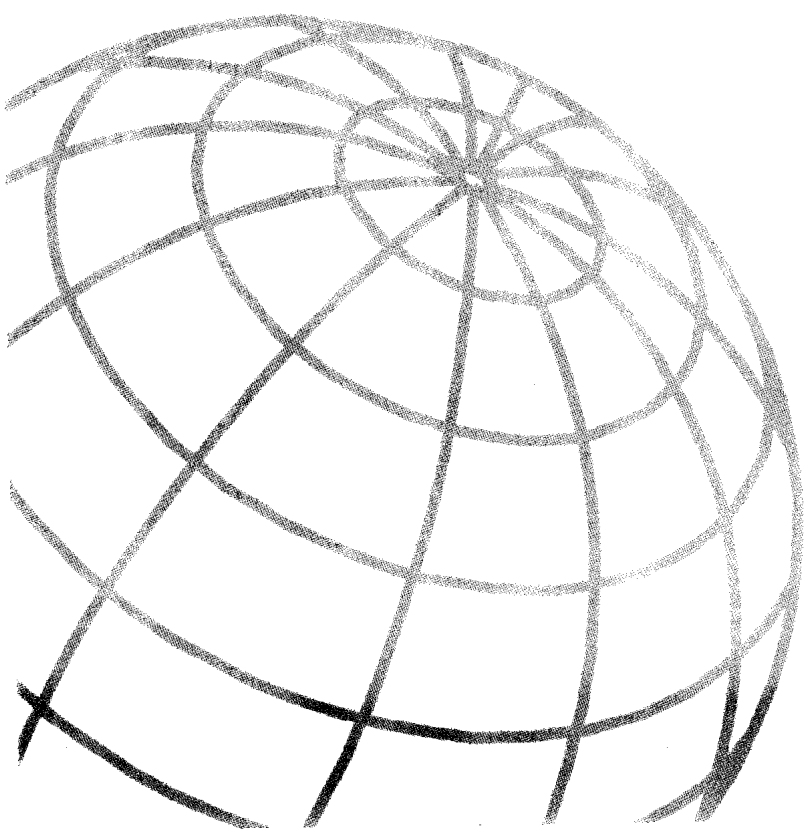
本丛书由中国信息安全产品测评认证中心组织编写，丛书的编写得到了何德全、周仲义、沈昌祥、蔡吉人几位院士的悉心指点，曲成义、方关宝、宁家骏、黄德根等专家更是为本书细心审校，业内相关人士尤其是首批 CISP 也给予了大力支持，在此一并表示感谢！

需要指出的是，由于丛书涉及内容较广，作者水平有限，书中难免会有疏漏之处，敬请专家和广大读者指正。

有关本丛书内容的更新更正以及参考资料信息，可查询：http://www.cisp.org.cn。

中国信息安全产品测评认证中心

2003 年 9 月



目 录

第 1 章　标准概述

1.1　标准和标准化的概念

1.1.1　标准和标准化定义

1．标准的定义

为在一定范围内获得最佳秩序，对活动或其结果规定共同的和重复使用的规则、导则或特性的文件。该文件经协商一致并由一个公认的机构批准。

注：标准应以科学技术和经验的综合成果为基础，以促进最佳社会效益为目的。

2．标准化的定义

为在一定的范围内获得最佳秩序，对实际或潜在的问题制定共同的重复使用的规则的活动。

注 1：上述活动主要是制定、发布及实施标准的过程。

注 2：标准化的重要意义是改进产品、过程或服务的适用性，防止贸易壁垒，并促进技术合作。标准化的总目的是为在一定范围内获得最佳秩序并促进最佳社会效益，除此之外，标准化还可以有一个或多个特定目的，以适应某种需要。

（1）品种控制：为满足主要需要，对产品、过程或服务的量值（如种类数量）的最佳选择。

（2）适用性：产品、过程或服务在特定条件下适合规定用途的能力。

（3）兼容性：在特定条件下，不同产品、过程或服务一起使用时，能满足有关要求，而不会引起不能接受的干扰的适应性。

（4）互换性：一种产品、过程或服务能满足同样要求的能力。

（5）安全：没有不可接受的伤害或损害的危险性。

（6）环境保护：保护环境免受由产品、过程或服务的影响和作用而造成的不能接受的损害。

（7）产品保护：保护产品在使用、运输或存储过程中免受气候或其他有害条件的损害。

1.1.2　标准化的对象及范围

1．标准化学研究的对象

标准化学研究的对象是标准化学的基本概念、支撑标准化学的理论基础、标准化原理、标准化形式、标准化系统、标准体系和标准化科学管理。

2．标准化工作的对象

标准化的对象主要是围绕成果、过程、行为和条件因素4个方面展开的。

（1）成果：指经过某种转换过程产生的成果，如产品、劳务和服务等。成果是标准化的最基本的对象。这样的标准包括产品标准、服务标准。

（2）过程：指成果赖以产生的转换过程及其构成部分，如生产过程、设计过程、工艺过程、流程过程、管理过程，以及这些过程所包含的阶段和作业。过程及其构成是标准化的又一个重要对象。这样的标准包括设计规程、供给规程和管理规程。

（3）行为：指人的活动。人是人类社会一切活动过程的主体。人的行为包含过程和动作，也存在程序和方法问题，这也是标准化的重要对象。这样的标准包括工作标准、操作规程。

（4）条件因素：指实现过程和取得预期成果所需要的条件因素，主要包括资源（原材料、能源、信息等）、装备（设备、设施等）、人员和环境等方面的条件，它们也是标准化的重要对象。这样的标准包括材料标准、设备标准、人员素质标准和环境条件标准。

为便于大家理解，下面具体以通信行业的标准化三维空间为例来反映标准化活动的领域及内容，如图1-1所示。

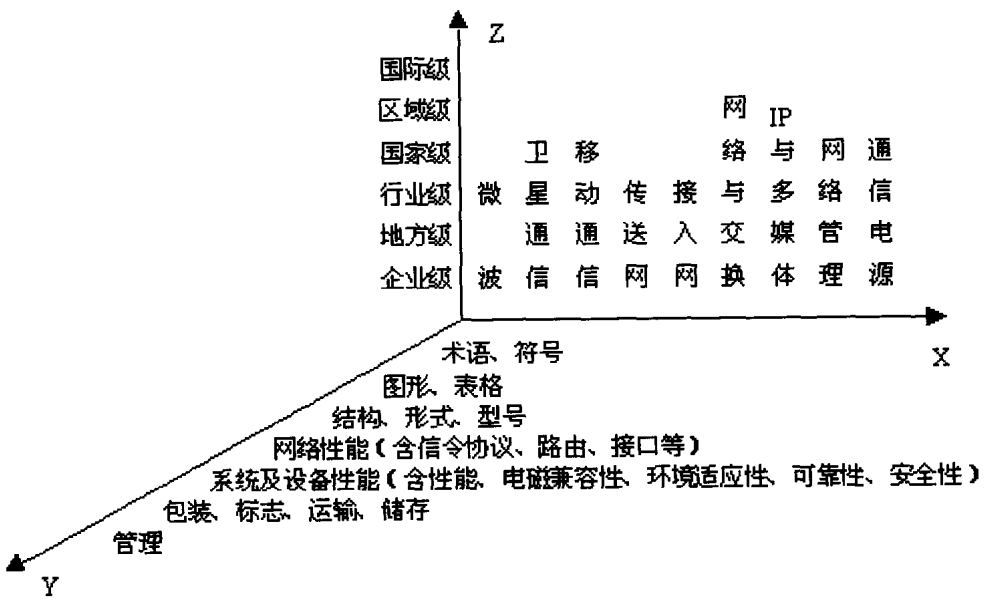


图1-1 标准化三维空间

*X*轴代表标准化领域，*Y*轴代表标准化的内容，*Z*轴代表标准化的级别。

1.1.3 标准化工作

1．制定标准

制定标准是指标准制定部门对需要制定标准的项目编制计划、组织草拟、审批、编号、发布的活动。它是标准化工作的任务之一，也是标准化活动的起点。

2．标准实施

标准实施是指有组织、有计划、有措施地贯彻执行标准的活动，是标准制定部门、使用部门或企业将标准规定的内容贯彻到生产、流通和使用等领域中去的过程。它是标准化工作的任务之一，也是标准化工作的目的。

3．标准实施的监督

对标准实施的监督是国家行政机关对标准贯彻执行情况进行督促、检查和处理的活动。它是政府标准化行政主管部门和其他有关行政主管部门领导和管理标准化活动的重要手段，也是标准化工作的任务之一，其目的是促进标准的贯彻，监督标准贯彻执行的效果，考核标准的先进性和合理性。通过标准实施的监督，随时发现标准中存在的问题，为进一步修订标准提供依据。

1.2　标准化的意义

- 标准化有利于发展社会主义市场经济。
- 标准化是促进科技进步的重要途径。
- 标准化能够保证产品、工程和服务质量。
- 标准化是提高企业管理水平的基础。
- 标准化是加强国际贸易与合作的有效工具。

1.3　标准化的发展

1.3.1　标准化的早期发展

标准化的历史虽可追溯到史前时代，并在公元 14 和 15 世纪已有许多辉煌成就，但在世界范围内把标准化作为一项自觉的有意识的活动，是 20 世纪初才开始的，至于在国家和国际范围内，设立专门机构，有组织、有计划地开展，则是第二次世界大战前后的事。1947 年国际标准化组织（ISO）成立时，各成员国已有 15 万个国家标准，ISO 当时的主要精力用于协调各成员国的标准。协调过程中遇到的种种问题，使 ISO 认识到理论建设的重要性，于是在 1952 年成立了标准化的原理委员会（ISO/STACO），并且作为 ISO 的常设机构，从世界各国聘任著名专家担任成员，其主要任务是从事标准化理论和方法的研究。在 ISO/STACO 的影响下，有些国家也成立了相应的研究机构。

1.3.2　标准化学科的理论基础

1972 年桑德斯（T.R.B.Sanders）（1963～1972 担任 ISO/STACO 主席）和松浦四郎（日本标准化原理研究常设委员会创始人、ISO/STACO 成员）分别出版了《标准化的目的原理》