



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



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

## 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

顾 问 何德全院士 周仲义院士  
沈昌祥院士 蔡吉人院士

主 编 吴世忠

副 主 编 徐铁夫 王贵驹 滕若波

编 委 江常青 赵明霄 张富民 张帆

执行编委	陈若兰	陈 洁	张 利	邹 琪	江典盛
	陈 捷	李 婧	万晓君	王洪琛	黄晓茜
	周丽波	付居周	木建华	张 杰	杨志刚
	史 蓉	王建国	董海波	王青石	汪宇昕
	冯 悦	李希衡	王 毅	余浩然	张艳军

主 审 曲成义 方关宝 宁家骏 黄德根

# 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。

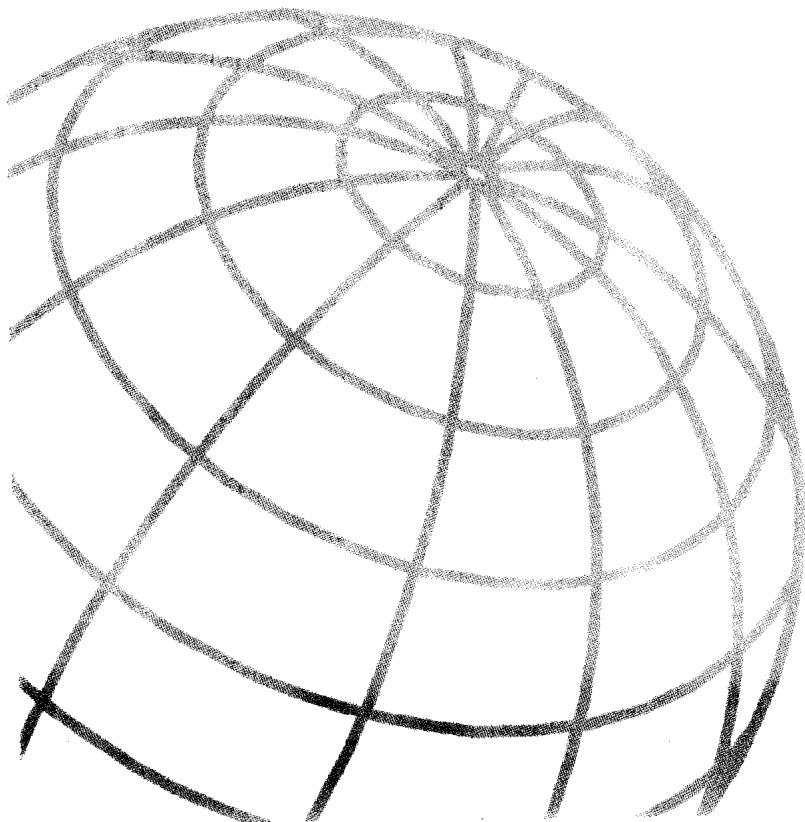
## 关于作者

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

<b>第 1 章 标准概述</b> .....	1
1.1 标准和标准化的概念 .....	1
1.1.1 标准和标准化定义 .....	1
1.1.2 标准化的对象及范围 .....	1
1.1.3 标准化工作 .....	2
1.2 标准化的意义 .....	3
1.3 标准化的发展 .....	3
1.3.1 标准化的早期发展 .....	3
1.3.2 标准化学科的理论基础 .....	3
1.3.3 世界经济及技术的新发展对标准化产生的影响 .....	4
1.3.4 信息技术标准的发展趋势 .....	5
1.4 国际通用“标准化七原理” .....	5
<b>第 2 章 国际标准发展概况</b> .....	7
2.1 信息技术标准化组织 .....	7
2.1.1 国际标准化组织 (ISO) .....	7
2.1.2 国际电工委员会 (IEC) .....	9
2.1.3 国际电信联盟 (ITU) .....	9
2.1.4 因特网工程任务组 (IETF) .....	10
2.1.5 欧洲计算机厂商协会 (ECMA) .....	10
2.2 ISO 9000 族简介 .....	11
2.2.1 ISO 9000 族标准的起源与发展 .....	11
2.2.2 ISO 9000 族标准的构成 .....	12
2.2.3 ISO 9000 质量管理体系的应用 .....	13
2.2.4 ISO 9000 族与信息技术安全性评估通用准则 (CC) 的关系 .....	14
2.3 因特网标准的发布 .....	14
2.3.1 因特网社团组织及责任 .....	14
2.3.2 RFC 的发布 .....	15
2.3.3 标准化进程 .....	15
2.3.4 非标准进入文档 .....	16
2.4 国外信息安全标准化现状简介 .....	16



<b>第3章 我国信息安全标准化概况</b> .....	<b>19</b>
3.1 我国标准化情况简介 .....	19
3.1.1 我国采用国际标准的原则及规定 .....	19
3.1.2 我国标准化现状和存在的问题 .....	20
3.1.3 我国今后标准化的重点工作 .....	21
3.2 我国信息安全标准化概况 .....	23
3.3 我国信息安全标准 .....	23
3.3.1 基础类标准 .....	23
3.3.2 物理安全标准 .....	25
3.3.3 系统与网络标准 .....	27
3.3.4 应用与工程标准 .....	27
3.3.5 管理标准 .....	28
3.4 我国信息标准化未来发展的趋势 .....	29
3.4.1 建立国家信息安全标准体系框架 .....	29
3.4.2 企业承担标准制定工作 .....	29
<b>第4章 基础信息安全标准指南</b> .....	<b>31</b>
4.1 概述 .....	31
4.1.1 信息系统的安全问题 .....	31
4.1.2 信息安全技术标准的目标 .....	34
4.1.3 信息系统实体 .....	35
4.1.4 信息安全标准体系结构 .....	36
4.2 安全体系结构标准 .....	37
4.2.1 安全体系结构的依据、目的和内容 .....	37
4.2.2 典型的网络安全体系结构标准 .....	37
4.3 安全框架标准指南 .....	41
4.3.1 安全框架标准概述 .....	41
4.3.2 组织结构 .....	42
4.3.3 通用概念 .....	51
4.3.4 一般的安全信息 .....	54
4.3.5 一般的安全业务 .....	56
4.3.6 业务的拒绝/操作的连续 .....	57
4.3.7 安全服务与安全机制在实现中的关系 .....	58
4.4 信息安全技术中的安全机制标准指南 .....	59
4.4.1 加密机制 .....	59
4.4.2 访问控制机制 .....	67
4.4.3 数据完整性机制 .....	70
4.4.4 鉴别机制 .....	71

4.4.5	数字签名机制 .....	74
4.4.6	抗抵赖机制 .....	76
4.4.7	路由选择控制机制 .....	77
4.4.8	公证机构 .....	77
4.4.9	普遍安全机制 .....	77
<b>第 5 章</b>	<b>环境与平台安全标准指南 .....</b>	<b>79</b>
5.1	电磁泄漏发射技术标准指南 .....	79
5.2	物理环境与保障标准 .....	80
5.2.1	计算机机房安全 .....	80
5.2.2	计算机场地安全 .....	80
5.2.3	电源与备份 .....	81
5.2.4	灾难预防与恢复 .....	82
5.2.5	电磁兼容 .....	82
5.3	计算机安全等级标准 .....	83
5.3.1	我国计算机安全保护等级划分准则 .....	83
5.3.2	美国国防部可信计算机评价准则 (TCSEC) .....	86
5.4	网络平台安全标准 .....	88
5.4.1	概述 .....	88
5.4.2	防火墙 .....	89
5.4.3	链路层加密 .....	89
5.4.4	基于 IPSec 的网络加密 .....	90
5.5	应用平台安全标准 .....	91
5.5.1	数据库安全 .....	91
5.5.2	Web 安全技术 .....	92
5.5.3	E-mail 安全技术 .....	93
5.5.4	文件传送系统安全技术 .....	94
5.5.5	SSH .....	95
5.5.6	电子商务标准 .....	96
5.5.7	文电处理系统安全保密 (X.400) 标准指南 .....	99
5.5.8	目录系统 (X.500) 安全服务标准指南 .....	103
5.5.9	IPV6 标准研究指南 .....	104
5.5.10	数据加密物理层互操作性要求 .....	106
5.5.11	简单网络管理协议 .....	109
<b>第 6 章</b>	<b>信息安全产品标准指南 .....</b>	<b>111</b>
6.1	密码模块安全标准 .....	111
6.1.1	概述 .....	111

6.1.2	密码模块的安全目标 .....	112
6.1.3	密码模块的安全要求 .....	113
6.1.4	系统安全级别的确定 .....	121
6.2	包过滤防火墙安全标准 .....	121
6.2.1	包过滤防火墙概述 .....	121
6.2.2	包过滤防火墙安全环境 .....	122
6.2.3	包过滤防火墙安全目标 .....	123
6.2.4	包过滤防火墙安全要求 .....	124
6.3	应用级防火墙安全标准 .....	125
6.3.1	应用级防火墙概述 .....	125
6.3.2	应用级防火墙安全环境 .....	126
6.3.3	应用级防火墙安全目标 .....	127
6.3.4	应用级防火墙安全功能要求 .....	128
6.4	路由器安全标准 .....	129
6.4.1	概述 .....	129
6.4.2	安全目标 .....	130
6.4.3	安全技术要求 .....	130
6.4.4	路由器安全功能要求 .....	131
6.4.5	路由器安全级别划分的建议规则 .....	132
6.5	安全 VPN .....	133
6.5.1	概述 .....	133
6.5.2	安全环境 .....	133
6.5.3	安全目标 .....	133
6.5.4	安全要求 .....	134
6.5.5	安全管理 .....	135
6.6	证书认证中心安全标准 .....	135
6.6.1	概述 .....	135
6.6.2	公钥体系 .....	135
6.6.3	认证中心适用范围 .....	141
6.6.4	管理要求 .....	142
6.6.5	运行要求 .....	144
6.6.6	系统和设施要求 .....	145
6.7	话音保密设备的安全要求 .....	146
6.8	数据保密设备的安全要求 .....	148
6.9	传真保密设备的安全要求 .....	149
6.10	安全 PC 卡 (PCMCIA 安全卡) .....	150
6.11	智能卡 .....	153

<b>第 7 章 信息安全管理标准</b> .....	155
7.1 信息安全管理简介 .....	155
7.2 我国信息安全管理面临的问题 .....	156
7.3 英国信息安全管理标准 BS7799 .....	157
7.3.1 BS7799 的发展 .....	157
7.3.2 使用 BS7799 标准建立信息安全管理体 系 .....	158
7.3.3 BS7799 的应用范围 .....	159
7.3.4 BS7799-2 结构的介绍 .....	159
<b>第 8 章 信息安全测评认证标准</b> .....	161
8.1 我国信息安全测评认证体系 .....	161
8.1.1 信息安全测评认证体系理论基础 .....	161
8.1.2 我国信息安全测评认证体系组织结 构 .....	162
8.3 信息技术安全测评标准的发展 .....	165
8.4 信息技术安全性评估通用准则 (CC) .....	168
8.4.1 CC 的主要用户 .....	168
8.4.2 评估环境 .....	169
8.4.3 CC 的组成 .....	169
8.4.4 CC 的特点 .....	176
8.4.5 CC 的国际互认 .....	177
8.5 我国信息技术安全性评估准则 (GB/T 18336) .....	177
8.5.1 GB/T18336 的适用范围 .....	177
8.5.2 GB/T 18336 的作用 .....	178
8.5.3 GB/T 18336 的目标读者 .....	178
8.5.4 文档组织 .....	179
8.5.5 关键概念 .....	179
8.5.6 安全功能要求和安全保证要求 .....	181
8.5.7 评估保证级和安全性评估 .....	184
8.6 信息系统安全工程能力成熟模型及其评 定方法 .....	188
8.6.1 SSE-CMM 的发展史 .....	188
8.6.2 SSE-CMM 的用途 .....	188
8.6.3 能力级别 .....	189
8.6.4 过程区 (PA) .....	191
8.6.5 过程区与安全工程过程 .....	192
8.6.6 SSE-CMM 的体系结构 .....	194
8.6.7 评定方法 .....	196
<b>第 9 章 信息安全法律法规概貌</b> .....	197

9.1	国际信息安全法律法规概要 .....	197
9.1.1	美国信息安全法律法规概要 .....	197
9.1.2	欧洲信息安全法律法规概要 .....	197
9.1.3	亚洲信息安全法律法规概要 .....	199
9.1.4	各国密码政策简介 .....	199
9.2	我国现有信息安全相关法律法规 .....	202
9.2.1	国家法律 .....	202
9.2.2	行政法规 .....	202
9.2.3	部门规章及规范性文件 .....	203
9.2.4	地方法律法规 .....	204
<b>第 10 章</b>	<b>我国信息安全法律法规 .....</b>	<b>205</b>
10.1	现有部分信息安全法律简介 .....	205
10.1.1	中华人民共和国宪法相关信息安全部分摘录 .....	205
10.1.2	中华人民共和国刑法相关信息安全的内容简介 .....	206
10.1.3	全国人大通过的维护互联网安全决定 .....	207
10.2	现有部分信息安全行政法规简介 .....	209
10.2.1	中华人民共和国计算机信息系统安全保护条例简介 .....	209
10.2.2	商用密码管理条例简介 .....	210
10.3	现有部分信息安全部门规章及规范性文件简介 .....	211
10.3.1	计算机信息网络国际联网安全保护管理办法简介 .....	211
10.3.2	计算机病毒防治管理办法简介 .....	212
10.3.3	计算机信息系统国际联网保密管理规定简介 .....	212
10.3.4	计算机信息系统安全专用产品检测和销售许可证管理办法简介 .....	212
<b>附录 A</b>	<b>缩略语和术语 .....</b>	<b>215</b>
一、	缩略语 .....	215
二、	术语 .....	216
<b>附录 B</b>	<b>信息安全法律法规 .....</b>	<b>227</b>
一、	国家法律 .....	227
	中华人民共和国保守国家秘密法 .....	227
	中华人民共和国标准化法 .....	230
	中华人民共和国产品质量法 .....	233
	中华人民共和国国家安全法 .....	241
	维护互联网安全的决定 .....	244
二、	行政法规 .....	245
	中华人民共和国产品质量认证管理条例 .....	245

中华人民共和国计算机信息系统安全保护条例 .....	249
中华人民共和国计算机信息网络国际联网管理暂行规定 .....	251
中华人民共和国计算机信息网络国际联网管理暂行规定实施办法 .....	252
商用密码管理条例 .....	256
三、部门规章及规范性文件 .....	259
计算机信息网络国际联网安全保护管理办法 .....	259
计算机病毒防治管理办法 .....	262
计算机信息系统国际联网保密管理规定 .....	264
互联网电子公告服务管理规定 .....	266
科学技术保密规定 .....	268
网上证券委托暂行管理办法 .....	272
计算机信息系统安全专用产品检测和销售许可证管理办法 .....	276
注册信息安全专业人员认证程序 .....	279



# 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。

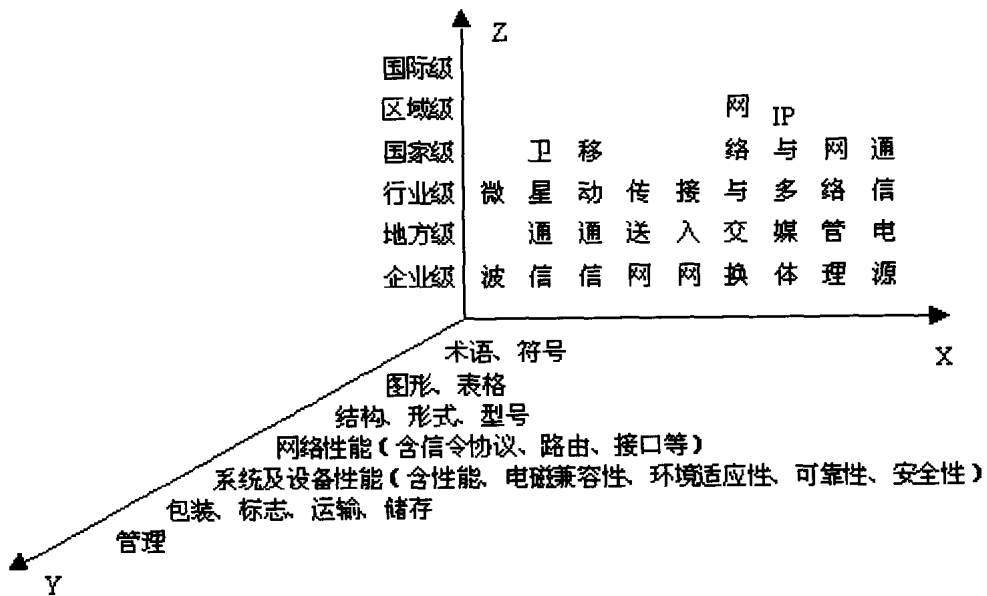


图 1-1 标准化三维空间

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》