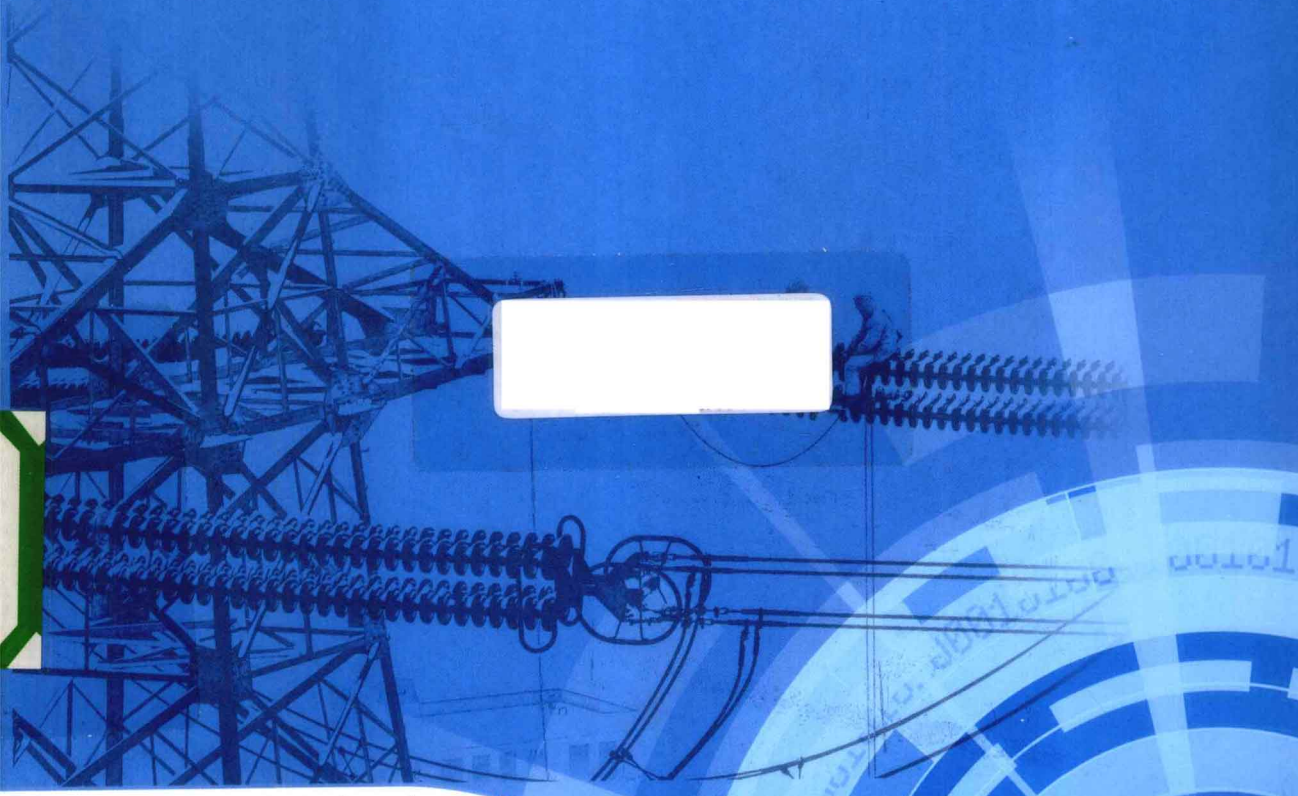
DIANLIHANGYE XINXIANQUAN
DENGJIBAOHU CEPING

电力行业信息安全等级保护测评

金 波 主编



中国电力出版社
CHINA ELECTRIC POWER PRESS

DIANLIHANGYE XINXIANQUAN
DENGJIBAOHU CEPING

电力行业信息安全等级保护测评

金 波 主编

中国电力出版社
CHINA ELECTRIC POWER PRESS

内 容 提 要

本书在研究分析国家信息安全等级保护有关管理要求和技术标准的基础上，总结近几年大量信息系统安全等级保护实施工作的经验，结合电力企业信息安全建设的特点，提出融合风险度量的信息安全等级保护测评技术。

本书共四篇18章，主要内容包括信息安全等级保护概述、信息系统安全等级保护测评基础、融合风险度量的测评技术、信息收集与分析方法、物理安全测评方法、主机安全测评方法、网络安全测评方法、应用安全测评方法、数据安全及备份恢复测评方法、管理安全测评方法、整体测评方法、信息安全评价体系概述、信息安全评价方法与指标、信息安全评价结果、测评准备、方案编制、现场测评、分析与报告编制。此外，附录部分提供了信息安全评价指标和信息调查表，以供参考。

本书理论结合实际，具有很强的可操作性，可供从事电力行业信息安全工作的技术人员和决策人员使用，也可供其他行业信息安全从业人员参考使用。

图书在版编目（CIP）数据

电力行业信息安全等级保护测评/金波主编. —北京：中国电力出版社，2013.2

ISBN 978-7-5123-3913-2

Ⅰ.①电… Ⅱ.①金… Ⅲ.①电力系统—信息安全 Ⅳ.①TM7

中国版本图书馆CIP数据核字（2013）第000261号

中国电力出版社出版、发行

（北京市东城区北京站西街19号 100005 http://www.cepp.sgcc.com.cn）

北京丰源印刷厂印刷

各地新华书店经售

*

2013年2月第一版 2013年2月北京第一次印刷

787毫米×1092毫米 16开本 21印张 499千字

印数0001—4000册 定价 **68.00**元

《电力行业信息安全等级保护测评》

编写人员名单

主　　编　金　波

编写人员　徐　晖　王　甜　黄敬志　魏理豪

钱　扬　王义申　刘　兰

序

随着信息技术的高速发展和网络应用的迅速普及，我国国民经济和社会信息化进程全面加快，信息系统的基础性、全局性作用日益增强，信息资源已经成为国家经济建设和社会发展的重要战略资源之一。保障信息安全，维护国家安全、公共利益和社会稳定，是当前信息化发展中迫切需要解决的重大问题。

公安部、国家保密局、国家密码管理局和国信办联合发布的《关于信息安全等级保护工作的实施意见》中明确了信息安全等级保护的核心是对信息安全分等级、按标准进行建设、管理和监督。

本书的编者是在信息安全技术、实践和管理领域工作多年的专家，对技术发展的脉络有着深刻的洞察力和远见。在充分学习和研究国家信息安全等级保护制度、标准的基础上，总结近几年大量信息系统安全等级保护实施工作的经验，提出融合风险度量的信息安全等级保护测评技术，在保证信息安全工作效率的基础上，更全面地管理和控制企业信息安全风险，切实提高企业信息安全的整体防护水平。

该书编写团队深入地开展了信息系统等级保护测评方法及关键技术的研究，进行了理论攻关、工程实践，结合等级保护测评结论，站在系统论的高度，提出一种基于等级保护测评结论的信息安全评价考核体系。该书对于意在开展信息安全等级保护实施工作的读者很有参考价值。

该书是近年来难得的信息系统安全等级保护方面的专著，尽管编者所提出的信息安全等级保护测评方法仍有待未来更多的实践检验，但其知新求变、融会贯通的思想是积极的。本书值得电力行业管理人员研读，对行业技术人员也会有所启迪。期待编者的团队在实践中进一步提高理论的可操作性，并进一步推动信息安全等级保护实施工作的发展。

中国科学院院士 陈国良

2012 年 11 月

前　言

信息系统安全等级保护测评是信息安全等级保护工作的关键内容，目前国家已发布的标准和方法主要对测评技术进行了规范和定义，在实际工作中依然存在大量的难点和需要进一步完善的方面。因此深入开展信息系统安全等级保护测评方法及关键技术的研究，进行理论攻关、工程实践，是开展信息安全等级保护安全建设、整改和测评工作的迫切需求，也是国家信息安全等级保护实施工作进一步落地的基础。

本书在对信息系统安全等级保护测评技术的相关标准进行研究，总结广东电网公司近几年在其实施工作过程中的实践经验，结合电力企业本身的信息安全建设特点，对该技术在实施过程中的主要方法和流程进行了全面介绍。同时，本书详细介绍了广东电网公司在工作过程中对等级测评技术所做的有益尝试，包括进一步引入信息安全风险评估技术中定量分析的风险度量方法，以及对等级测评结果数据深入挖掘所总结的信息安全评价体系，为读者全面掌握等级测评技术提供帮助。

本书分四篇，包括信息系统安全等级保护测评基础、电力行业信息系统安全等级保护测评实践、电力行业信息系统安全评价体系和电力行业信息系统安全等级保护测评案例分析。第 1 篇（第 1、2 章）简单介绍了国家信息安全等级保护工作实施的背景，对等级保护各主要环节的工作内容进行了阐述；第 2 篇（第 3～11 章）介绍了融合风险度量的测评技术，并以典型信息系统为例，详细介绍了各安全领域的测评技术方法，包括物理安全、主机安全、网络安全、应用安全、数据安全与备份恢复以及管理安全测评技术方法；第 3 篇（第 12～14 章）阐述了建立企业内部的信息安全评价体系的意义，并详细介绍了如何建立信息安全评价体系；第 4 篇（第 15～18 章）以办公自动化系统为例，详细介绍了等级保护测评实施的全过程，帮助读者更好地理解前三篇的内容。

信息系统安全等级保护测评工作是信息安全的新领域，无论是在测评理论研究，还是在测评具体实践上，都对信息安全工作人员提出了新的挑战。本书介绍的测评方法已经在电网企业中进行了有效实践，但还存在一定的局限性，不同企业开展等级测评实施工作时，可结合本行业、本企业的实际情况，制订相应的实施计划和测试方案，不宜生搬硬套。

在本书编写过程中，中国科学院陈国良院士为编写给予了指导，广州竞远系统网络技术有限公司（胡斌先生等）提供了大量的支持和帮助，在此一并表示深切地感谢。

本书所涉及的内容大都具有尝试性和探索性，与此相关的许多理论和实际问题还需要进一步深入研究，限于编者的水平，书中难免有疏漏和不当之处，恳请广大专家和读者批评指正。

本书编写组

2013 年 2 月

目 录

第 4 篇 电力行业信息系统安全等级保护测评案例分析

第 1 篇

信息安全等级保护测评基础

随着信息技术的飞速发展和网络技术的广泛应用，全球信息化步伐在不断加快，但信息系统自身暴露的脆弱性，导致政府和企业的信息安全事件频发，比如伊朗布什尔核电站计算机遭到“震网”病毒攻击、索尼云计算服务网站遭到黑客攻击等。正因为信息安全形势日益严峻，信息安全问题逐渐凸显，世界各国已将信息安全作为国家安全和经济安全事务中的重要工作之一，尤其是构建可信的网络、建设有效的信息安全保障体系、实施切实可行的信息安全保障措施已经成为世界各国信息化发展的主流需求。

目前，信息安全等级保护已成为发达国家保护关键信息基础设施、保障信息安全的通行做法，同时也是我国多年信息安全工作经验的总结。开展信息安全等级保护工作不仅是保障重要信息系统安全的重大措施，也是一项事关国家安全、社会稳定、国家利益的重要任务。

在具体实施等级保护过程中，无论是作为此项工作推动者的政府主管部门、作为此项工作落实者的信息系统运营使用单位，还是为此项工作提供咨询和测评服务的第三方机构，都应该认真学习、领会等级保护政策和相关标准体系要求，避免信息系统安全等级保护工作出现不符合国家标准的情况、出现落实不细致和不完备等情况。本篇作为基础篇章，主要介绍了信息安全等级保护产生的背景、相关的标准体系以及开展信息安全等级保护工作的概要，让读者对此有一个大体的了解。

第1章 信息安全等级保护概述

1.1 国外相关研究

美国的信息安全研究一直走在世界前列。近年来在计算机信息系统安全方面，突出体现了系统分类分级实施保护的发展思路，对国家一些重要的信息系统实现了安全分级、不同管理的工作模式，并形成了体系化的标准和指导性文件。在20世纪80年代，美国国防部就有针对性地开展了一系列工作。于1983年公布了可信计算机系统评估准则TCSEC（Trusted Computer System Evaluation Criteria，俗称橘皮书），后来成立了美国国家计算机安全中心（NCSC）进行有关工作，于1987年出版了一系列有关可信计算机的指南等（俗称彩虹系列）。彩虹系列从网络安全的角度出发，解释了TCSEC中的观点，从用户登录、授权管理、审计跟踪、隐通道分析、可信通道建立、安全检测、生命周期保障、文本写作、用户指南均提出了规范性要求，将安全等级分为D、C1、C2、B1、B2、B3和A1 7个级别，开创了分等级保护的先河。

20世纪90年代，西欧四国（英、法、荷、德）联合提出了技术安全评估标准（Information Technology Security Evaluation Criteria，ITSEC）。ITSEC除了吸收美国TCSEC的成功经验外，还首次提出了保密性、完整性、可用性的概念，把可信计算的概念提高到可信技术的高度上来认识。他们的工作成为欧共体安全计划的基础，并对国际安全的研究、实施带来深刻的影响。

1995年，在前期的国际信息安全分级测评认证标准的基础上，由与TCSEC、ITSEC、(Canadian Trusted Computer Product Evaluation Criteria) CTCPEC和相关的6个国家7个相关政府组织开始联合行动，将各自独立的准则集合成一系列单一的、能被广泛接受的IT国际通用安全准则（CC）。1999年，CC准则成为国际标准（ISO/IEC 15408），该标准吸收了各先进国家对现代系统安全的经验与知识，对未来安全的研究与应用带来重大影响。

国外在信息安全分等级保护方面做的大量研究和实践，为我国推行等级保护工作奠定了良好的基础，提供了有益的经验。

1.2 我国信息安全等级保护制度

1.2.1 等级保护制度的重要意义

近年来，在党中央、国务院高度重视和全社会的共同努力下，我国网络信息安全工作取得了很大发展。但是我国信息安全工作起步晚，基础薄弱，网络信息安全面临的形势依然十分严峻。这主要体现在以下4个方面。

(1) 社会对网络信息内容安全的认识虽然已普遍提高，但对网络系统自身的安全性却认识不足。一些企业片面地认为内部使用的网络信息就是安全的，因而缺乏网络安全保护意识和能力。随着信息化发展特别是电子政务的建设，互联互通和信息共享已越来越广泛，单位内部网络信息

面临的安全威胁越来越大。特别是集中在党政机关以及金融、电信、能源、交通运输等重要部门和企业，这些关系国计民生的网络信息如果遭到外部攻击或内部破坏，后果将十分严重。

（2）网络系统安全建设和管理存在很大的盲目性。大多数单位不清楚如何建设网络系统才是安全的。有的人认为，安装了防火墙、防病毒、入侵检测等安全设备的网络就是安全的。这种低水平的安全建设和管理，不仅使建设投资缺乏针对性，而且也难以保证网络的整体安全防范能力。

（3）对网络信息安全保护工作的监测管理薄弱。近年，我国出台了多部网络信息安全的法律法规和技术标准，赋予多个主管部门在网络信息领域行使监督执法职能，但随着信息技术的迅猛发展和我国信息化进程的加快，传统的管理方式越来越不适应。执法主体不集中，多重管理和多头管理比较普遍，对重要程度不同的网络信息的管理要求没有差异、没有标准，缺乏针对性。

（4）规范化、高水平的网络信息安全服务市场还未形成。由于网络信息安全的专业性强，专门人才有限，而社会上专业化程度高、专门从事网络安全技术咨询、风险分析、检测评估等业务的网络安全服务机构极为缺乏，难以为全社会提供足够的网络安全技术支持和服务。因此，我国绝大多数单位的网络信息基本上是自主建设、自行管理，安全防范和管理服务水平很低。

如何全面和整体解决各行各业在信息化建设中的安全问题，是国内外信息安全领域多年来一直关注的问题。西方发达国家为了抵御网络信息的脆弱性和安全威胁，已经制定了一系列强化网络信息安全建设的政策和标准。在制定政策和标准的时候，其中一个很重要的思想就是将按照安全保护强度划分不同的安全等级，以指导不同领域的信息安全工作，在制定网络信息安全政策和标准的时候也借鉴了这一思路。因此，实行等级保护是在借鉴国外先进经验和结合我国国情的基础上解决我国网络信息安全的必然选择。我国通过实施安全等级保护，可以转变政府职能，强化国家监管，进一步明确单位、企业和个人责任，积极推动网络信息安全服务机制的建立和完善，最终有效地解决我国网络信息安全问题。

1.2.2 信息安全等级保护制度的确立

党中央、国务院高度重视信息安全保障工作。1994 年国务院颁布的同国务院令第 147 号《中华人民共和国计算机信息系统安全保护条例》规定，“计算机信息系统实行安全等级保护。安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”，要求实行安全等级保护。1999 年，国家质量技术监督局正式发布了强制性国家标准 GB 17859—1999《计算机信息系统　安全保护等级划分准则》。

2003 年 7 月，国家信息化领导小组第三次会议专门研究信息安全问题，审议通过中办发〔2003〕27 号《国家信息化领导小组关于加强信息安全保障工作的意见》，提出了今后一段时期我国信息安全保障工作的总体要求和主要原则，首次明确了信息安全等级保护制度是我国信息安全保障工作的基本制度。

1.2.3 信息安全等级保护标准

为推动我国信息安全等级保护工作，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制定了信息安全等级保护工作需要的一系列标准，形成了比较完整的信息安全等级保护标准体系（见图 1-1）。

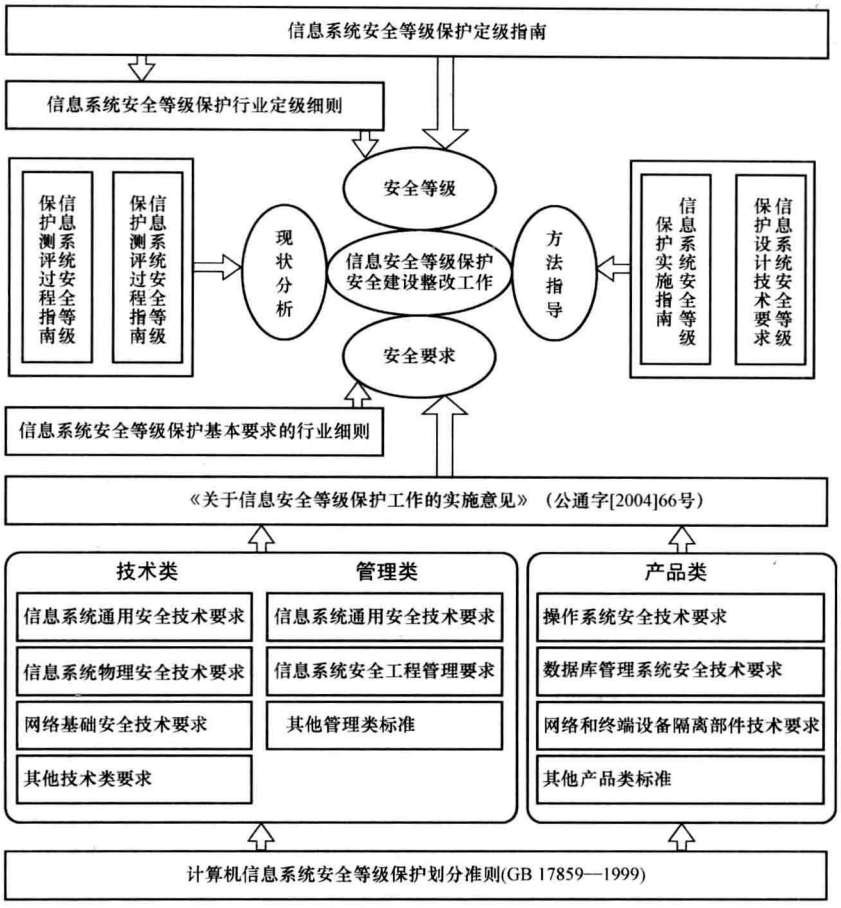


图 1-1　信息安全等级保护标准体系

信息安全等级保护相关标准大致可以分为基础类、应用类、产品类和其他类四类，具体见表 1-1。

表 1-1　　信息系统安全等级保护相关标准

标准分类	子类型	标　准　名　称
基础类	—	GB 17859—1999《计算机信息系统　安全保护等级划分准则》
应用类	信息系统定级	GB/T 22240—2008《信息安全技术　信息系统安全等级保护定级指南》
	等级保护实施	信安字〔2007〕10 号《信息安全技术　信息系统安全等级保护实施指南》
	信息系统安全建设	GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》
		GB/T 20271—2006《信息安全技术　信息系统通用安全技术要求》
		GB/T 25070—2010《信息安全技术　信息系统等级保护安全设计技术要求》
		GB/T 20269—2006《信息安全技术　信息系统安全管理要求》
		GB/T 20282—2006《信息安全技术　信息系统安全工程管理要求》
		GB/T 21052—2007《信息安全技术　信息系统物理安全技术要求》
		GB/T 20270—2006《信息安全技术　网络基础安全技术要求》
		GA/T 708—2007《信息安全技术　信息系统安全等级保护体系框架》
		GA/T 709—2007《信息安全技术　信息系统安全等级保护基本模型》
		GA/T 710—2007《信息安全技术　信息系统安全等级保护基本配置》

续表

标准分类	子类型	标 准 名 称
应用类	等级测评	GB/T 28448—2012《信息安全技术　信息系统安全等级保护测评要求》
		GB/T 28449—2012《信息安全技术　信息系统安全等级保护测评过程指南》
		GA/T 713—2007《信息安全技术　信息系统安全管理测评》
产品类	操作系统	GB/T 20272—2006《信息安全技术　操作系统安全技术要求》
		GB/T 20008—2005《信息安全技术　操作系统安全评估准则》
	数据库	GB/T 20273—2006《信息安全技术　数据库管理系统安全技术要求》
		GB/T 20009—2005《信息安全技术　数据库管理系统安全评估准则》
	网络	GB/T 20279—2006《信息安全技术　网络和终端设备隔离部件安全技术要求》
		GB/T 20277—2006《信息安全技术　网络和终端设备隔离部件测试评价方法》
		GB/T 20278—2006《信息安全技术　网络脆弱性扫描产品技术要求》
		GB/T 20280—2006《信息安全技术　网络脆弱性扫描产品测试评价方法》
		GA/T 684—2007《信息安全技术　交换机安全技术要求》
		GA/T 686—2007《信息安全技术　虚拟专用网安全技术要求》
	PKI	GA/T 687—2007《信息安全技术　公钥基础设施安全技术要求》
		GB/T 21053—2007《信息安全技术　公钥基础设施 PKI 系统安全等级保护技术要求》
	网关	GA/T 681—2007《信息安全技术　网关安全技术要求》
	服务器	GB/T 21028—2007《信息安全技术　服务器安全技术要求》
	入侵检测	GB/T 20275—2006《信息安全技术　入侵检测系统技术要求和测试评价方法》
		GA/T 700—2007《信息安全技术　计算机网络入侵分级要求》
	防火墙	GA/T 683—2007《信息安全技术　防火墙安全技术要求》
		GB/T 20281—2006《信息安全技术　防火墙技术要求和测试评价方法》
		《信息安全技术　信息系统安全等级保护防火墙安全配置指南》
		GB/T 20281—2006《信息安全技术　防火墙技术要求和测试评价方法》
		GB/T 20010—2005《信息安全技术　包过滤防火墙评估准则》
	路由器	GB/T 18018—2007《信息安全技术　路由器安全技术要求》
		GB/T 20011—2005《信息安全技术　路由器安全评估准则》
		GA/T 682—2007《信息安全技术　路由器安全技术要求》
	交换机	GB/T 21050—2007《信息安全技术　网络交换机安全技术要求（评估保证级 3）》
		GA/T 685—2007《信息安全技术　交换机安全评估准则》
	其他产品	GA/T 671—2006《信息安全技术　终端计算机系统安全等级技术要求》
		GB/T 20945—2007《信息安全技术　审计产品技术要求和测试评价方法》
		GB/T 20979—2007《信息安全技术　虹膜识别系统技术要求》
		GA/T 686—2007《信息安全技术　虚拟专用网安全技术要求》
		GA/T 711—2007《信息安全技术　应用软件系统安全等级保护通用技术指南》
		GA/T 712—2007《信息安全技术　应用软件系统安全等级保护通用测试指南》
		GB/T 20277—2006《信息安全技术　网络和终端设备隔离部件测试评价方法》
		GB/T 20280—2006《信息安全技术　网络脆弱性扫描产品测试评价方法》

续表

标准分类	子类型	标 准 名 称
其他类	风险评估	GB/T 20984—2007《信息安全技术　信息安全风险评估规范》
	事件管理	GB/Z 20985—2007《信息技术　安全技术　信息安全事件管理指南》
		GB/Z 20986—2007《信息安全技术　信息安全事件分类分级指南》
		GB/T 20988—2007《信息安全技术　信息系统灾难恢复规范》

下面对表 1-1 中的等级保护的几个重要标准进行简要介绍。

一、等级划分准则

GB 17859 是强制性国家标准，也是等级保护的基础性标准。国家在此基础上制定出 GB/T 20271—2006 等技术类和 GB/T 20269—2006、GB/T 20282—2006 等管理类以及 GB/T 20272—2006 等产品类标准，在相关标准的制定时起到了奠定作用。

该标准按照信息系统安全保护能力划分了用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级、访问验证保护级共 5 个级别。从自主访问控制、强制访问控制、标记、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、可信恢复 10 个方面，采取逐级增强的方式提出可计算信息系统的安全保护技术要求。其主要用于规范和指导计算机信息系统安全保护相关标准的制定，为安全产品的研究开发提供技术支持，为计算机信息系统安全法规的制定和执法部门的监督检查提供依据。

二、等级保护基本要求

GB/T 22239—2008 是在 GB 17859—1999、技术类标准和管理类标准的基础上，总结几年的实践，结合当前信息技术发展的实际情况研究制定的。该标准提出了各级信息系统应当具备的安全保护能力，并从技术和管理两方面提出了相应的措施。电力行业按照 GB/T 22239—2008 等国家标准，结合行业特点，结合系统安全保护的特殊需求，在公安部等有关部门指导下，制定了自己行业的标准规范和细则。

GB/T 22239—2008 提出了各种信息系统应当具备的安全保护能力，并从技术和管理两方面提出了相应的措施，为信息系统建设单位和运营使用单位在系统安全建设中提供参照。该标准的技术部分采纳了 GB 17859—1999 及相关标准中的身份鉴别、数据完整性、自主访问控制、强制访问控制、审计、剩余信息保护、标记、可信路径 8 个安全机制，并将这些机制根据各级的安全目标，扩展到网络层、主机系统层、应用层和数据层，主要划分为物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复 5 个方面。而管理部分则借鉴了 ISO/IEC 17799：2005 等国际上流行的信息安全管理方面的标准，划分为安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理 5 个方面。

三、等级保护定级指南

GB/T 22240—2008 为确定信息系统安全保护等级提供支持。该标准规定了定级的依据、对象、流程和方法以及等级变更等内容，用于指导开展信息系统定级工作。电力行业按照 GB/T 22240—2008 等国家标准，结合行业特点和信息系统的特殊性，在公安部等有关部门的指导下，制定行业信息系统定级规范或细则。

GB/T 22240—2008 依据《信息系统安全等级保护管理办法》（简称《管理办法》），从信息系统对国家安全、经济建设、社会生活的重要作用，信息系统承载业务的重要性以及业务对信息系统的依赖程度等方面，提出确定信息系统安全保护等级的方法。其内容包括了定

级原理、定级方法以及等级变更等。

四、等级保护实施指南

《信息系统安全等级保护实施指南》（简称《实施指南》）主要阐述了等级保护实施的基本原则、参与角色和信息系统定级、总体安全规划、安全设计与实施、安全运行与维护、信息系统终止等几个主要工作阶段中如何按照信息安全等级保护政策、标准要求实施等级保护工作。

《管理办法》第九条规定，信息系统运营、使用单位应当按照《实施指南》具体实施等级保护工作。《实施指南》用于指导信息系统运营使用单位，在信息系统从规划设计到终止运行的过程中如何按照信息安全等级保护政策、标准要求实施等级保护工作。

五、安全设计技术要求

GB/T 25070—2010 提出了信息系统等级保护安全设计的技术要求，包括第一～第五级信息系统安全保护环境的安全计算环境、安全区域边界、安全通信网络和安全管理中心等方面的设计技术要求，以及定级系统互联的设计技术要求，明确了体现定级系统安全保护能力的整体控制机制，可用于指导信息系统运营使用单位、信息安全企业、信息安全服务机构等开展信息系统等级保护安全技术设计。

六、等级保护测评要求及过程指南

GB/T 28448—2012 和 GB/T 28449—2012 构成了指导开展等级测评的标准规范。等级保护测评要求阐述了等级测评的原则、测评内容、测评强度、单元测评要求、整体测评要求、等级测评结论的产生方法等内容，用于规范和指导测评人员如何开展等级测评工作。过程指南阐述了信息系统等级测评的测评过程，明确了等级测评的工作任务、分析方法以及工作结果等，包括测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动，用于规范测评机构的等级测评过程。

根据《管理办法》的规定，信息系统建设完成后，运营使用单位或者其主管部门应当选择符合规定条件的测评机构，依据 GB/T 28448—2012 等技术标准，定期对信息系统安全等级状况开展等级测评。GB/T 28448—2012 依据 GB/T 22239—2008 规定了对信息系统安全等级保护进行安全测试评估的内容和方法，用于规范和指导测评人员的等级测评活动。

GB/T 28449—2012 则明确了信息系统等级测评的测评过程，阐述了等级测评的工作任务、分析方法以及工作结果等，为信息系统测评机构、运营使用单位及其主管部门在等级测评工作中提供指导。

1.2.4 信息安全等级保护基本原则

2004 年 9 月 15 日，由公安部、国家保密局、国家密码管理局和国信办联合下发《关于信息安全等级保护工作的实施意见》，明确信息安全等级保护的核心是对信息安全分等级按标准进行建设、管理和监督。信息安全等级保护实施工作应遵循以下基本原则。

一、明确责任，共同保护

通过等级保护，组织和动员国家、法人和其他组织、公民共同参与信息安全保护工作；各方主体按照规范和标准分别承担相应的、明确具体的信息安全保护责任。

二、依照标准，自行保护

国家运用强制性的规范及标准，要求信息和信息系统按照相应的建设和管理要求，自行