http://www.phei.com.cn

信息系统等级保护安全建设技术方案设计实现与应用

◎ 胡志昂　主编
◎ 范　红　执行主编

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

信息系统等级保护安全建设技术方案设计实现与应用

胡志昂　主　　编

范　红　执行主编

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

国家标准 GB/T 24856－2009《信息安全技术　信息系统等级保护安全设计技术要求》是根据我国信息安全等级保护的实际需要，按照信息安全等级保护对信息系统安全整改的要求制定的，对信息系统等级保护安全整改阶段技术方案的设计具有指导和参考作用。本书对该标准进行了详细的解读，以帮助读者学习和理解该标准。

本书涵盖了信息系统等级保护安全体系结构、关键技术、等级保护模拟平台、信息系统等级保护安全建设方案及应用案例等方面的内容。针对信息系统等级保护安全建设工作中需要解决的各类问题，本书为读者提供从理论到实践的帮助，并为广泛开展信息系统等级保护安全建设工作提供指导。

图书在版编目（CIP）数据

信息系统等级保护安全建设技术方案设计实现与应用/胡志昂主编. —北京：电子工业出版社，2010.2
ISBN 978-7-121-10262-2

Ⅰ.信… Ⅱ.胡… Ⅲ. 信息系统—安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2010）第 012135 号

策划编辑：周　琰
责任编辑：周　琰　　特约编辑：寇国华
印　　刷：涿州市京南印刷厂
装　　订：涿州市桃园装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：880×1 230　1/16　印张：29.25　字数：948 千字
印　　次：2010 年 2 月第 1 次印刷
定　　价：98.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

编委会名单

前　言

信息安全等级保护是我国实现国家信息安全的基本制度，1994 年国务院 147 号令中就已规定信息系统安全实行等级保护制度，并明确指出由公安部会同有关部门制定等级保护管理办法和标准；1999 年国家发布了等级保护强制性国家标准 GB 17859－1999《计算机信息系统安全保护等级划分准则》，此后，50 多个配套标准相继发布，并已形成标准体系。这些标准的制定，为信息安全等级保护制度的实施打下了坚实的技术基础。2003 年 27 号文件则进一步明确规定国家实施信息安全等级保护制度，此后，公安部等四部委联合相继发布了 66 号和 43 号文件，规定了等级保护系列政策和管理办法。

2007 年 7 月，重要信息系统等级保护定级工作会议的召开，标志着等级保护制度在全国范围内全面展开。目前，全国重要信息系统定级工作已基本完成。下一阶段的工作将对已确定安全等级的信息系统依据相关标准要求进行安全建设。此工作将涉及大量的关键技术实现难题，因此，深入开展信息系统等级保护安全体系结构及关键技术的研究，进行理论攻关、工程实践与标准制定，是即将开展的信息系统等级保护安全建设整改工作的迫切现实需要，也是国家信息安全等级保护制度长期实施所不可缺少的技术支持。

国家标准 GB/T 24856－2009《信息安全技术　信息系统等级保护安全设计技术要求》是根据我国信息安全等级保护的实际需要，按照信息安全等级保护对信息系统安全整改的要求制定的，对信息系统等级保护安全整改阶段技术方案的设计具有指导和参考作用。本书对该标准进行了详细地解读，以帮助读者学习和理解该标准。

本书涵盖了信息系统等级保护安全体系结构、关键技术、等级保护模拟平台、信息系统等级保护安全建设方案及应用案例等方面的内容。针对信息系统等级保护安全建设工作中需要解决的各类问题，我们尽最大可能为读者提供从理论到实践的帮助，以期为广泛开展的信息系统等级保护安全建设工作提供指导。

编　者

目　录

第 1 章

信息安全等级保护及其发展状况

信息安全等级保护可以简单地理解为通过划分等级的方法实现保护信息安全的目标。由于安全保护主要针对信息系统的存储、传输和处理的数据信息，所以从信息系统安全方案设计的角度，本书将信息安全等级保护称为“信息系统等级保护”。

划分等级的方法是指将涉及信息安全的相关内容和方法划分为不同等级，以实现不同的安全保护目标。其中信息安全保护的相关内容和方法包括对数据信息进行存储、传输和处理的信息系统的安全保护所采用的安全技术措施和安全管理措施。

划分等级的方法可以分为两大类，一类是从技术角度划分，另一类是从管理角度划分。二者的根本区别在于从技术角度划分主要以信息安全的基本要素为单位，对实现相应安全功能的安全技术和机制提出不同要求；从管理角度划分主要是以信息系统的安全为目标，对实现不同安全要求的信息系统提出不同要求。从实施信息安全等级保护制度出发，由于作为最终目标的信息安全是通过对信息和信息系统的安全保护实现的，所以从技术角度或管理角度进行安全等级划分，进而为实现不同安全等级信息系统的安全保护提供支持。当然对于没有实施信息安全等级保护制度的情况，从技术角度所进行的安全等级划分对于研究和区别不同安全技术和机制所实现的具有不同安全等级的信息安全产品，进而合理地使用这些产品同样具有十分重要的意义和作用。这就是为什么在国外虽然没有把信息安全等级保护作为一项制度，但仍然对信息安全技术和产品进行安全等级划分的原因。

在国外，最早的信息安全标准是美国国防部推出的《可信计算机系统评估准则》（TCSEC），以及由此产生的一系列从技术角度进行等级划分的信息安全标准。这种类型的标准对信息安全所进行的等级划分，其主要特点是以信息安全的要素作为划分安全等级的基本单位。不同安全等级对各个安全要素有不同的要求，从而确定不同安全产品的不同安全等级。我国最早的信息安全分等级标准 GB 17859—1999《计算机信息系统安全保护等级划分准则》也是从技术的角度进行等级划分，它根据我国信息安全技术发展的实际情况，以 TCSEC 为基本参考确定了 10 个安全要素并按这些安全要素对计算机信息系统的安全保护等级进行划分。显然随着信息技术和信息安全技术的发展，这 10 个安全要素已经远远不能覆盖当前信息系统所涉及的信息安全问题。

我国当前所实施的信息安全等级保护制度是从管理角度进行等级划分的典型代表，公通字［2004］66 号文件和公通字［2007］43 号文件关于对信息和信息系统进行等级划分的描述是从管理角度对信息和信息系统进行的等级划分，或者说是根据信息和信息系统对安全保护的需求进行的等级划分。如果说中办［2003］27 号文件确定了信息安全等级保护作为我国实现国家信息安全的一项基本制度的话，那么在这之前我国所制定的一些标准主要是从技术角度进行安全等级划分，而在此之后则转变为从管理角度进行安全等级划分。按照我国信息安全等级保护制度的要求，从管理角度划分安全等级所涉及的内容应该涵盖从技术角度划分安全等级的内容。因为一项制度的实施既要有管理方面的措施，也需要有技术方面的支持。从管理角度划分安全等级的要求主要体现在信息安全的有关政策法规中，而从技术角度划分安全等级的要求则主要体现在信息安全的相关标准中。

需要指出的是，到目前为止，把信息安全等级保护明确规定为一项实现国家信息安全的制度在国外

还不多见。所以说，我国当前所实行的信息安全等级保护制度是一种具有创新性和挑战性的工作。如果说我国是通过实施信息安全等级保护制度，采用对信息系统进行分等级管理的方法实现信息系统的安全保护，那么国外普遍采用的则是通过风险管理的方法来实现信息系统的安全保护。这两种实现信息系统安全保护的管理方法都需要按照从技术角度进行安全等级划分所提供的不同安全等级的安全技术和安全产品的支持，因为重点保护和适度保护的思想无论对于哪一种管理方法都是适用的。

由于信息安全技术与信息技术是密不可分的，所以信息安全技术所反映的特性也称为“信息技术的安全性”。信息安全技术的发展寓于信息技术的发展之中，信息安全等级保护是信息安全的组成部分，所以本章关于信息安全等级保护及其发展状况的描述只能是对信息技术、信息安全技术和信息安全等级保护及其发展状况的统一描述。

本章将从信息安全发展简介、理解和认识我国信息安全等级保护，以及国外信息安全等级划分等方面说明信息安全等级保护及其发展状况。

1.1 信息安全发展简介

1.1.1 信息安全发展的基本情况

信息安全是一个具有悠久历史的话题，随着阶级的出现人们就开始注意信息的保密，早在古罗马时代就用简单的密码来隐蔽信息。国家的出现，使政治、经济、军事及外交等领域的信息安全成为十分重要的问题。在早期，除了采用物理和管理措施以外，用密码技术来隐蔽信息成为信息传送中最有效的保护手段。

20 世纪 40 年代以来，计算机的出现和计算技术的迅速发展使信息的存储、传输和处理形式发生了巨大变化。随着计算机在社会各个领域的广泛应用，以计算机为核心的信息安全问题越来越突出地表现出来。与计算机出现以前的信息安全保密相比，计算机信息系统的安全保密问题要多得多，也复杂得多，涉及从物理环境到硬件、软件、系统运行，以及数据传输等各个方面。除了传统的安全保密技术外，计算机信息系统的安全有丰富的内容和完整的体系。

20 世纪 70 年代以来，以网络为平台的信息处理系统迅速发展，使计算机从应用发展到网络阶段，也使人类社会步入信息时代。网络化的信息系统是集计算机、通信和信息处理于一体，连接广大区域的系统，是现代社会活动不可缺少的基础。随之而来的信息安全问题也更加复杂化，由单一计算机系统的信息安全变成包括计算机系统在内，以及大量与网络相关的环境、传输及体系结构等相关的系统安全问题。系统安全包括系统安全运行和信息安全保护两个方面，涉及计算机安全、网络安全、操作安全、访问控制、物理安全、电磁安全，以及法律和管理等方面的内容。20 世纪 70 年代以来是密码技术蓬勃发展的时期，并随着应用的推广逐步走向社会并走向大众。

20 世纪 90 年代以来，信息系统安全以信息安全保障为目标，在保密性和完整性的基础上强调可用性要求的实现。密码技术则向集成化发展，PKI（Public Key Infrastructure，公钥基础设施）技术是其典型代表；另外，密码技术与信息系统安全的结合是当前信息安全的一个重要发展局势。综合系统安全技术与密码技术，信息安全技术的发展可以粗略地划分为以下 3 个阶段。

第 1 阶段：以通信信息保护为主要内容，以单一密码技术为主要技术手段，计算机安全技术与通信安全技术分离。

第 2 阶段：以信息的保密性、完整性及真实性保护为主要内容，密码技术向多元化发展。以访问控制为核心的系统安全技术得到发展，计算机安全技术与通信安全技术相结合。

第 3 阶段：系统安全技术以安全保障（保密性、完整性及可用性）为主要内容，密码技术向集成化

发展。计算机安全技术与通信安全技术密切结合，密码技术与系统安全技术密切结合。

标准是技术发展的产物，同时又推进技术的发展，信息安全标准也不例外。信息安全标准的发展在一定程度上可以反映信息安全技术的发展情况，20 世纪 80 年代初制定的《可信计算机系统评估准则》（TCSEC）成为推进信息安全的经典之作。此后，欧洲各国、加拿大及澳大利亚等在安全技术发展的基础上相继推出了各自的信息安全标准（包括 1988 年德国的《绿皮书》；1989 年英国的《信息安全标准》，1991 年英国、德国、法国及荷兰等国联合制定的《供欧洲共同体使用的信息技术安全评估准则》（ITSEC），1993 年加拿大的《可信计算机产品评估准则》（CTCPEC），以及 1993 年美国的《安全联邦标准草案》（FC）等），并在此基础上于 1998 年上述相关国家和部门共同制定出反映当前信息安全技术发展的最新标准——ISO/IEC 15408：1999 Information technology-Security techniques-Evaluation Criteria for IT Security（信息技术-安全技术-IT 安全性评估准则，简称 CC）。这些充分反映了信息安全技术从 20 世纪 80 年代后期以来，在世界范围内得到广泛重视和迅速发展。

我国信息安全技术在近年来也得到迅速发展，随着信息化步伐的加快，信息安全问题显得越来越突出，信息安全受到广泛关注。在业内人士的共同努力下，我国信息安全技术已经取得了长足的进步，IDS、防火墙及防病毒等安全产品随处可见并在信息系统的安全防范方面发挥了积极的作用。在有关部门的推动下，已经发布并正在制定的一系列信息安全技术标准对于促进信息系统的安全建设和安全产品的开发起到了积极的推动作用。但是由于我国信息安全技术的基础还十分薄弱，与信息安全技术密切相关的芯片、操作系统及数据库管理系统等信息技术和产品还是国外产品占领主要市场。当前我国信息安全从技术到管理，还远远不能适应信息化发展的需要。这一切表明，我国信息安全任重而道远。需要全国同仁共同奋斗，尽早实现信息安全，为信息化保驾护航的目标。

1.1.2　信息安全的新发展

20 世纪 90 年代以来，信息安全方面有许多新的发展，主要表现在观念上的转变、认识上的提高，以及技术上的进步等方面。

1．观念上的转变

安全观念上的转变主要是指信息安全的概念由信息安全保护发展为信息安全保障的转变，信息安全保障所包含的信息保护、运行检测、快速反应及故障恢复等，对于信息系统安全来说并非都是新的内容。但在新的环境和情况下能更全面并更完整地反映现代信息系统对信息安全要求的新变化，即更加关注信息系统所提供的安全可靠的服务。人们已经不只是采用被动的保护手段来进行信息安全防护，而是从服务的角度，从系统的高度来提供可信、完整、一致且可靠的信息服务的保障。从一定意义上讲，这种信息安全保障的概念已经涵盖了从使用角度对信息系统的所有要求。

2．认识上的提高

认识上的提高主要表现在以下三方面。

（1）安全的相对性原理

安全的相对性原理主要是指任何一个信息系统的安全性都是相对的，没有绝对安全的系统。因为安全与攻击、破坏及一切不安全行为之间是一种对抗的关系，是矛与盾的关系，所谓“道高一尺，魔高一丈”就是这个道理。当然相对安全应该是有标准的，所以当我们说某一个系统或某些信息是安全的，只能理解为该系统符合一定的安全等级要求，或者该信息受到某种程度的安全保护。安全的相对性原理对于了解和建立安全信息系统都是十分重要的，更是认识和理解信息安全等级保护思想的基础。

（2）安全整体性和木桶原理

安全的整体性是指一个信息系统的安全性应从整体及系统的角度考虑，系统安全性的木桶原理是指