ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28452—2012

信息安全技术
应用软件系统通用安全技术要求

Information security technology—
Common security technique requirement for application software system

2012-06-29 发布　　2012-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京江南天安科技有限公司、北京思源新创信息安全资讯有限公司。

本标准主要起草人:吉增瑞、陈冠直、王志强、景乾元。

引　言

本标准描述为实现 GB 17859—1999 所规定的每一个安全保护等级的应用软件系统应达到的安全技术要求，为按照信息系统安全等级保护的要求设计和实现所要求的安全等级的应用软件系统提供指导。

从广义角度，应用软件系统应该包括针对特定应用开发的业务处理软件，以及为这些业务处理软件的开发和运行提供支持的各种工具软件和中间件等。本标准仅对各个安全保护等级的业务处理软件的安全保护应采取的安全技术进行描述。

应用软件系统是信息系统的重要组成部分，是信息系统中对应用业务进行处理的软件的总和。业务应用的安全需求，是信息系统安全需求的出发点和归宿。信息系统安全所采取的一切技术和管理措施，最终都是为确保业务应用安全的。这些安全措施，有的可以在应用软件系统中实现，有的需要在信息系统的其他组成部分实现。

本标准主要是对各个应用领域的应用软件系统普遍适用的安全技术要素的安全技术要求的描述。不同应用领域的应用软件系统可选取不同的安全技术要素，以满足各自应用业务的具体安全需求。本标准同时对应用软件系统生存周期的各个阶段应遵循的安全技术要求进行了简要描述。

按照标准编写的规范性要求，本标准在第 1 章范围、第 2 章规范性引用文件及第 3 章术语和定义、缩略语之后，第 4 章应用软件生存周期安全技术要求，从应用软件生存周期的角度，分别对应用软件的开始阶段、获得或开发阶段、实现和评估阶段、运行和维护阶段以及结束和处置阶段的安全技术要求进行了简要描述。标准从第 5 章到第 9 章，以 GB 17859—1999 的五个安全等级的划分为基本依据，以 GB/T 20271—2006 关于信息系统通用安全技术要求的等级划分为基础，对每一个安全等级的应用软件系统的安全技术要求进行了描述，包括：安全功能技术要求和安全保证技术要求（含应用软件系统安全子系统自身保护要求、应用软件系统安全子系统设计和实现要求、应用软件系统安全子系统安全管理要求）。在第 5 章到第 9 章的分等级描述中，“**加粗宋体**”表示在较高等级中比较低一级增加或增强的内容。本标准附录 A（资料性附录）应用软件系统安全的有关概念说明，对应用软件系统在信息系统中的位置和应用软件系统安全在信息系统安全中的作用等进行了说明。附录 B（资料性附录）应用软件系统安全与信息系统安全的关系，对应用软件系统安全是信息系统安全的核心和应用软件系统安全需求就是信息系统安全需求进行了描述。附录 C（资料性附录）给出了应用软件系统安全要素与安全分等级要求之间的对应关系。表 C.1 是安全功能技术要素与安全功能技术分等级要求的对应关系；表 C.2 是安全保证技术要素与安全保证技术分等级要求的对应关系。

信息安全技术
应用软件系统通用安全技术要求

1 范围

本标准规定了按照GB 17859—1999的5个安全保护等级的划分对应用软件系统进行等级保护所涉及的通用技术要求。

本标准适用于按照GB 17859—1999的5个安全保护等级的划分对应用软件系统进行的安全等级保护的设计与实现。对于按照GB 17859—1999的5个安全保护等级的划分对应用软件系统进行的安全等级保护的测试、管理也可参照使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 20272—2006 信息安全技术 操作系统安全技术要求

GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求

3 术语和定义、缩略语

3.1 术语和定义

GB/T 20271—2006界定的以及下列术语和定义适用于本文件。

3.1.1

应用软件系统 application software system

信息系统的重要组成部分，是指信息系统中对特定业务进行处理的软件系统。

3.1.2

应用软件系统安全技术 application software system security technology

为确保应用软件系统达到确定的安全性目标的安全技术措施中可采用的技术。

3.1.3

应用软件系统安全子系统(SSOASS) security subsystem of application software system

应用软件系统中安全保护模块的总称。它建立了应用软件系统的一个基本安全保护环境，并提供安全应用软件系统要求的附加用户服务。按照GB 17859—1999对可信计算基(TCB)的定义，SSOASS属于应用软件系统的TCB。其中所需要的硬件和固件支持由低层的安全机制提供。

3.1.4

SSOASS安全策略(SSP) SSOASS security policy

对SSOASS中的资源进行管理、保护和分配的规则。一个SSOASS中可以有一种或多种安全策略。