ICS 35.020
L 09

GA

# 中华人民共和国公共安全行业标准

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

**Information security technology—**
**Common technique guide of security classification protection for application software system**

2007-08-13 发布　　2007-10-01 实施

中华人民共和国公安部　　发布

# 目　　次

# 前　言

本标准的附录A为资料性附录。

本标准由公安部信息系统安全标准化技术委员会提出并归口。

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、王志强、陈冠直、景乾元、宋健平。

# 引　言

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

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的安全。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概括描述。不同应用领域的应用软件系统应根据需要选取不同的安全技术要素，以满足其各自业务应用的具体安全需求。

本标准第 4 章，应用软件系统基础安全技术要求，是对应用软件系统的每一个安全等级都适用的基础性安全技术要求的描述，包括：应用软件系统风险分析和安全需求，应用软件系统安全方案，应用软件系统环境安全，应用软件系统业务连续性，以及应用软件系统与相应信息系统安全等级划分等。

本标准第 5 章，应用软件系统安全技术分等级要求，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描述，包括：基础安全技术要求，安全功能技术要求，以及为实现上述安全技术要求应用软件系统安全子系统的自身保护、设计和实现及安全管理要求。其中，“**加粗宋体**”表示在较高等级中比上一级增加或增强的内容。

# 信息安全技术
# 应用软件系统安全等级保护通用技术指南

## 1 范围

本标准规定了按照 GB 17859—1999 的五个安全保护等级的划分对应用软件系统进行安全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 的五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 的五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

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 20270—2006 信息安全技术 网络基础安全技术要求

GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求

GB/T 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、定义和缩略语

GB/T 20271—2006 确立的以及下列术语和定义适用于本标准。

### 3.1 术语和定义

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所采取的安全技术措施。

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装置的总称。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。