



中华人民共和国公共安全行业标准

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

Information security technology—
Common test 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	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 应用软件系统安全技术测试环境和条件要求	1
4.1 测试环境	1
4.2 测试条件	1
5 应用软件系统安全技术测试各安全等级共同要求	1
6 应用软件系统基础安全技术测试	2
6.1 风险分析和安全需求测试	2
6.2 应用软件系统安全方案测试	2
6.3 应用软件系统环境安全测试	2
6.4 应用软件系统业务连续性测试	2
6.5 应用软件系统及相关信息系统安全等级划分测试	2
7 应用软件系统安全技术分等级测试	2
7.1 第一级 用户自主保护级	2
7.1.1 安全技术测试环境和条件要求	2
7.1.2 基础安全技术测试	2
7.1.3 安全功能测试	3
7.1.4 SSOASS 自身保护测试	3
7.1.5 SSOASS 设计和实现测试	3
7.1.6 SSOASS 安全管理测试	4
7.2 第二级 系统审计保护级	4
7.2.1 安全技术测试环境和条件要求	4
7.2.2 基础安全技术测试	4
7.2.3 安全功能技术测试	4
7.2.4 SSOASS 自身保护测试	5
7.2.5 SSOASS 设计和实现测试	5
7.2.6 SSOASS 安全管理测试	6
7.3 第三级 安全标记保护级	6
7.3.1 安全技术测试环境和条件要求	6
7.3.2 基础安全技术测试	6
7.3.3 安全功能技术测试	6
7.3.4 SSOASS 自身保护测试	7
7.3.5 SSOASS 设计和实现测试	8
7.3.6 SSOASS 安全管理测试	8
7.4 第四级 结构化保护级	8

7.4.1	安全技术测试环境和条件要求	8
7.4.2	基础安全技术测试	8
7.4.3	安全功能技术测试	9
7.4.4	SSOASS 自身保护测试	10
7.4.5	SSOASS 设计和实现测试	10
7.4.6	SSOASS 安全管理测试	11
7.5	第五级 访问验证保护级	11
7.5.1	安全技术测试环境和条件要求	11
7.5.2	基础安全技术测试	11
7.5.3	安全功能技术测试	11
7.5.4	SSOASS 自身保护测试	12
7.5.5	SSOASS 设计和实现测试	13
7.5.6	SSOASS 安全管理测试	13

前 言

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

本标准对应用软件系统安全等级保护的测试提供指导,对应用软件系统所采用的安全技术是否达到其相应安全保护等级的要求进行测试。

本标准第 4 章,应用软件系统安全技术测试环境和条件要求,是对应用软件系统安全技术测试的环境的要求和应用软件系统安全技术测试所应具备条件的要求。

本标准第 5 章,应用软件系统安全技术测试各安全等级共同要求,是对应用软件系统的每一安全等级都适用的安全技术测试要求的描述。

本标准第 6 章,应用软件系统基础安全技术测试,是对 GA/T 711—2007 第 4 章所描述的应用软件系统的基础安全技术的测试。

本标准第 7 章,应用软件系统安全技术分等级测试,以 GA/T 711—2007 第 5 章关于应用软件系统安全技术分等级要求为基础,对每一个安全等级的应用软件系统的安全技术的测试要求的描述,包括:安全技术测试的环境和条件要求,基础安全技术测试要求,安全功能技术测试要求,以及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的测试要求。其中,“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。

信息安全技术

应用软件系统安全等级保护通用测试指南

1 范围

本标准规定了按照 GB 17859—1999 的五个安全保护等级对应用软件系统的安全保护等级进行测试的要求。

本标准适用于按照 GB 17859—1999 的五个安全保护等级的要求所进行的应用软件系统安全技术的测试。对于按照 GB 17859—1999 的五个安全保护等级对应用软件系统进行的安全设计和管理也可参照使用。

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

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

3 术语、定义和缩略语

GA/T 711—2007 中确立的术语、定义和缩略语适用于本标准。

4 应用软件系统安全技术测试环境和条件要求

4.1 测试环境

应用软件系统安全技术测试环境应满足以下要求：

- a) 支持应用软件系统运行的信息系统的其他各层的软、硬件(如物理层、网络层、操作系统层、数据库管理系统层等)均应具有不低于该应用软件系统的安全保护等级的安全性；
- b) 按照关联/互补的原则，应用软件系统的安全要求可以在应用软件系统中实现，也可以在支持其运行的低层环境中实现；
- c) 对应用软件系统的测试应在其实际运行环境或与实际运行环境相同的模拟环境进行；
- d) 应用软件系统中涉及密码的部分，应提供具有相应安全强度/等级的密码设施支持。

4.2 测试条件

被测应用软件系统应满足以下条件：

- a) 设计者应先进行自测试，并提供相应的测试文档和测试结果；
- b) 按照设计者所提供的测试文档所进行的测试，应能够再现设计者所做的自测试过程；
- c) 测试者可以根据应用软件系统所应达到的安全要求，进行新的测试；
- d) 涉及密码强度/等级的测试，应由国家密码主管部门按照相应的规定进行；
- e) 测试者根据对测试结果的分析，应能够对被测应用软件系统是否达到所需要的安全保护等级作出评价。

5 应用软件系统安全技术测试各安全等级共同要求

SSOASS 的开发者应提供包含每一个被测列项测试结果的自测试文档。自测试文档应说明被测列