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

中华人民共和国公共安全行业标准

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 711—2007

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230　1/16　印张 2.5　字数 66 千字
2007年11月第一版　2007年11月第一次印刷

*

书号:155066·2-18281　定价 28.00 元

GA/T 711-2007

GA/T 711—2007

中华人民共和国公安部　发布

附　录　A
（资料性附录）
应用软件系统安全的有关概念说明

A.1　应用软件系统在信息系统中的位置

应用软件系统位于信息系统最上层，与用户直接打交道。应用软件系统是在信息系统的硬件系统、操作系统、网络系统、数据库管理系统的支持下运行的，是构成信息系统的最重要部分，是信息系统中直接为用户提供服务的部分。上述其他系统都是为应用软件系统的运行提供支持和服务的。应用软件系统在信息系统中的位置如图 A.1 所示。

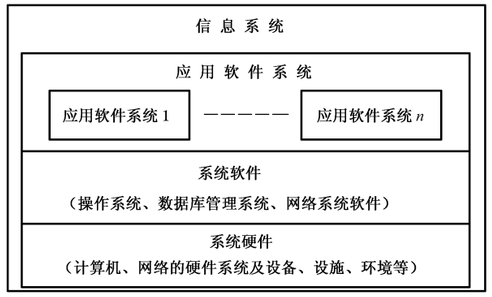

图 A.1　应用系统在信息系统中的位置

A.2　应用软件系统安全在信息系统安全中的作用

应用软件系统的安全是信息系统安全的重要组成部分。应用软件系统的安全需求是信息系统安全需求的来源和基础。为了实现应用软件系统的安全，需要有支持应用软件系统运行的硬件系统、操作系统、网络系统、数据库管理系统等各层安全的支持。应用软件系统的安全需求，根据具体情况，可以在应用软件系统层实现，也可以在支持应用软件系统运行的各层的支持下实现。

A.3　关于应用软件系统的业务连续性

应用软件系统的业务连续性是信息系统所承载的业务应用的连续性的表征，是信息系统安全运行的重要组成部分，通过应用软件系统的连续运行来支持。为对抗信息系统发生灾难性故障（比如：水灾、火灾、地震或严重的外部攻击等），使信息系统发生灾难性故障时能在限定的时间范围内恢复运行，业务连续性需要通过灾难备份与恢复来确保。与一般的安全性概念不同的是，对灾难备份与恢复的要求仅仅与信息系统所承载的业务的连续性要求有关，不同的业务应用有不同的业务连续性要求，从而有不同的灾难备份与恢复要求。其中的两个重要因素是数据备份的间隔时间和业务中断的时间。数据备份的时间间隔与允许数据丢失的程度有关，允许数据丢失的程度越小，数据备份的时间间隔就应越小；允许业务中断的时间间隔与业务停止运转所造成的损失有关，业务中断所造成的损失越大，允许业务中断的时间间隔就越小。

需要指出的是，业务连续性要求的分级与信息系统的安全等级并没有严格的对应关系。因为两者的依据是不一样的。但是，一般来讲，低等级安全要求的信息系统，业务连续性要求往往较低，所以在灾难备份与恢复方面的要求也就比较低，而高等级安全要求的信息系统，业务连续性要求往往较高，所以灾难备份与恢复方面的要求也就较高。

目　　次

b） 对防止误用的评定，应通过对文档的检查和分析确认，查找 SSOASS 以不安全的方式进行使用或配置而不为人们所察觉的情况；

c） 对 SSOASS 安全功能强度评估，应通过对安全机制的安全行为的合格性或统计结果的分析，证明其达到或超过安全目标要求所定义的最低强度；

d） **高抵抗力分析**，应通过独立穿透测试和对脆弱性的系统化搜索和完备性分析，确定 SSOASS 可以抵御**高攻击能力攻击者发起的穿透性攻击**。

5.5.5 SSOASS 安全管理

应根据本安全等级中安全功能技术要求所涉及的基础安全技术要求、安全功能技术要求和安全保证技术要求所涉及的 SSOASS 自身保护、SSOASS 设计和实现等有关内容，按 **GB/T** 20271—2006 中 6.5.6 的要求，从以下方面实现 SSOASS 的安全管理：

a） 对安全保证措施所涉及的 SSOASS 自身保护、SSOASS 设计和实现等有关内容，以及与一般的安装、配置等有关的功能，制定相应的操作、运行规程和行为规章制度；

b） 对 SSOASS 中的每个安全功能模块，根据安全功能技术和安全保证技术所实现的安全功能，实现 SSF 安全功能的管理；

c） 对 SSOASS 中的每个安全功能模块，根据安全功能技术和安全保证技术所涉及的安全属性，从管理安全属性、安全的安全属性、静态属性初始化、安全属性终止和安全属性撤消等方面，实现 SSF 安全属性的安全管理；

d） 对 SSOASS 中的每个安全功能模块，根据安全功能技术和安全保证技术所涉及的安全数据，从管理 SSF 数据、SSF 数据界限的管理和安全的 SSF 数据等方面，实现 SSF 安全数据的安全管理；

e） 将应用软件系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按最小授权原则分别授予他们各自为完成自身任务所需的最小权限，并形成相互制约的关系；

f） 对网络环境运行的应用软件系统，实现 SSOASS 安全机制的集中管理。