ICS 35.020
L 09

GA

中华人民共和国公共安全行业标准

GA/T 708—2007

信息安全技术
信息系统安全等级保护体系框架

**Information security technology—
Architecture framework of security classification
protection for information 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、附录B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

信息系统安全等级保护通过三大功能和五个环节，对国家、社会、集团和个人所建立和使用的信息系统，分等级实施必要的安全保护。

实现信息系统安全等级保护的三大功能是：

——防范与保护功能：从物理、网络、系统、应用和管理等组成部分，实现整体防范与保护；

——监督与检查功能：各单位自我检查与政府职能部门监督检查相结合，从技术和管理两个方面，确保信息系统的安全性达到确定安全等级的要求；

——响应与处置功能：信息系统拥有者，对系统的安全事件应有快速响应与处置的能力，并在发现重大问题时能及时向主管部门反映，与有关单位沟通。

实现信息系统安全等级保护的五个环节是指：

——政策、法规环节：制定完善的信息安全等级保护政策、法规，建立专门的管理机构，明确实施的程序和方法。

——规范化技术与管理环节：制定符合国情的信息系统安全等级保护技术和管理标准，并按标准要求实施安全管理，进行安全技术和产品的研究和开发。

——系统构建过程控制环节：按照谁主管谁负责的要求，对安全信息系统的构建过程进行全方位控制，并通过检测机构严格的检测评估，确保所构建的安全信息系统达到所需要的安全性要求。

——系统运行过程控制环节：按照谁运营谁负责的要求，对安全信息系统的运行过程进行全方位控制，并通过职能部门的监督检查，确保所运行的安全信息系统达到所设计的安全性要求。

——系统监督、检查环节：信息安全相关职能部门，依照法律、法规和标准，制定完善信息安全监管规章制度，开展信息安全等级保护专项管理工作。督促安全等级保护责任制的落实，监督、检查并指导信息系统所属部门和单位的信息系统安全等级保护的建设和管理，对安全技术产品实行监管，对安全检测机构实施监管。建立非盈利的覆盖全国的系统安全等级保护执法检查与检测支持体系，使用统一标准对运行中的安全信息系统进行检查、检测、评估，确保其实际运行过程中的安全性达到设计的目标要求。

本标准是对信息系统安全等级保护各个组成部分及其相互关系的描述，首先对信息系统安全等级保护的组成部分的主要内容及其相互关系做简要说明，然后对每一个组成部分的主要内容做比较详细的说明。

信息安全技术
信息系统安全等级保护体系框架

1 范围

本标准规定了按照信息安全等级保护的要求从技术角度对信息系统实施安全等级保护的体系框架。

本标准适用于按照信息系统安全等级保护所规定的五个安全保护等级的要求对信息系统实施安全等级保护所进行的技术活动及其相关的管理活动。

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

3 术语和定义

GB 17859—1999 确立的以及下列术语和定义适用于本标准。

3.1

安全信息系统 security information system

采用具有相应安全强度/等级的信息安全产品、信息安全技术和管理措施，以系统化方法设计和实现的，按照信息系统安全等级保护的要求具有一级/二级/三级/四级/五级安全性的信息系统。

3.2

信息安全系统 information security system

信息系统安全子系统的简称。一个信息系统的安全子系统是指由该信息系统中所有安全装置组成的系统。在 GB 17859—1999 中，将系统内保护装置的总体称为 TCB(可信计算基)。这里用信息安全系统的称谓是为了强调对信息系统的安全应以系统化的方法进行设计。

3.3

信息安全产品 information security production

具有确定安全强度/等级，用于构建安全信息系统的信息产品。信息安全产品分为信息技术安全产品和信息安全专用产品。信息技术安全产品是对信息技术产品附加相应的安全技术和机制组成的产品(如安全路由器)；信息安全专用产品是专门为增强信息系统的安全性而开发的信息安全产品(如防火墙)。

3.4

局域计算环境 local computing environment

由一个或多个计算机系统(主机/服务器)组成的，以对信息系统中的数据信息进行存储、处理为主要目的、有明确边界的计算环境。一个局域计算环境可以由一个计算机系统组成，也可以由多个计算机系统经局域网连接组成。

3.5

安全局域计算环境 security local computing environment

具有确定安全保护等级的局域计算环境。