ICS 35.020
L09

GA

中华人民共和国公共安全行业标准

GA/T 710-2007

信息安全技术
信息系统安全等级保护基本配置

Information security technology-
Fundamental configure 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

（略）

引　　言

信息系统安全等级保护的基本配置是从系统角度对信息系统安全等级保护的各个安全保护等级的安全机制配置的描述。

本标准给出了每一个安全保护等级的信息系统安全的基本配置，分别从局域计算环境安全及其分等级安全机制配置、局域计算环境边界防护及其分等级安全机制配置、用户环境安全及其边界防护分等级安全机制配置、网络系统安全及其分等级安全机制配置、安全域之间互操作安全机制配置、密码安全机制分等级配置、安全管理配置等方面，对各自安全的总体要求和分等级安全机制配置进行了说明。

信息安全技术
信息系统安全等级保护基本配置

1 范围

本标准规定了按照GB 17859-1999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每一个安全等级的基本配置。

本标准适用于按照GB 17859-1999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，每个安全等级各项安全机制的设计。

2 规范性引用文件

下列文件中的有关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 20269-2006 信息安全技术 信息系统安全管理要求

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

GA/T 708-2007 信息安全技术 信息系统安全等级保护体系框架

GA/T 709-2007 信息安全技术 信息系统安全等级保护基本模型

3 术语和定义

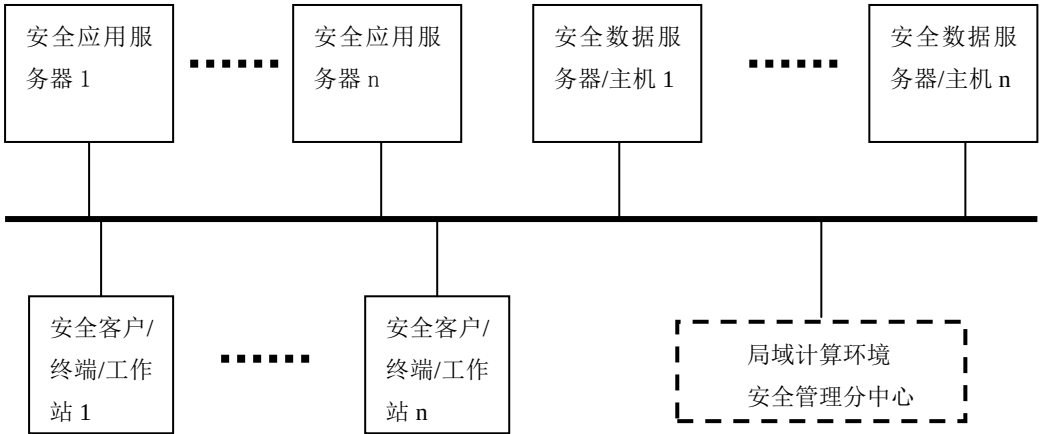
GA/T 708-2007确立的术语和定义适用于本标准。

4 信息系统安全等级保护基本配置

4.1 局域计算环境安全及其分等级安全机制配置

4.1.1 安全局域计算环境的组成与结构

安全局域计算环境的一般组成与结构如图1所示。



按图 1 所示，安全的局域计算环境是由安全的局域网络连接的各个安全的计算资源所组成的计算环境。其工作方式可以是客户/服务器模式、主机/终端模式、服务器/工作站模式，或者某种混合模式。

各种模式的具体组成分别为：

——客户/服务器模式:数据服务器、应用服务器、客户机、安全管理分中心及局域网络；

——服务器/工作站模式:服务器、工作站、安全管理分中心及局域网络；

——主机/终端模式:主机、终端、安全管理分中心及局域网络

——混合模式:由上述两种以上模式组成的局域计算环境。

4.1.2 总体要求

局域计算环境安全总的目标要求是，按所要求的安全保护等级，通过对局域计算环境各组成部分安全机制的配置和集成，保护局域计算环境中的数据信息不被非授权的泄露和破坏，保护局域计算环境安全运行，提供有效的服务。

局域计算环境的安全包括：

——对应用服务器、数据服务器/主机中数据的安全保护；

——客户机/工作站/终端对主机或服务器的安全访问；

——用户数据在局域网中的安全传输；

——在局域网中用户间数据的安全交换。

为此，安全应用服务器、安全数据服务器/主机均应配置具有相应安全保护等级的安全操作系统和安全数据库管理系统，以及具有相应安全保护等级的应用软件系统。安全客户/终端/工作站也应根据需要配置相应安全保护等级的操作系统和应用软件系统等安全的软件系统。安全局域网应通过对网络各层协议和网络设备的安全要求，达到数据在局域网中传输和交换的安全要求。

在具有较高安全保护等级的信息系统中应设置安全管理中心（必要时，在局域计算环境设置安全管理分中心）。局域计算环境安全管理分中心是对本局域计算环境实施安全管理的机构，与安全管理中心协同工作，实现对本局域计算环境的安全管理。它既是管理机构，又具有强烈的技术色彩。其中的各个安全管理机构的主要功能是收集和管理本局域计算环境的各类与安全相关的信息，经初步汇集后传送到信息系统安全管理控制中心，并按照安全管理中心的总要求对本局域计算环境实施安全管理。

随着安全保护等级的提高，局域计算环境的安全要求分别从安全机制配置的增加、安全强度的增强和安全管理措施的加强等方面有所体现。以下仅从安全机制配置方面对不同安全等级加以说明。按 GA/T 708-2007 中 8.3.2.2 的描述，以资产价值和威胁确定的信息系统安全保护等级，是对信息系统的局域计算环境进行分等级安全机制配置的基本依据。

4.1.3 局域计算环境分等级安全机制配置

4.1.3.1 一级安全机制

按 GA/T 709-2007 中图 2 所给出的具有一级安全的信息系统安全基本模型，根据局域计算环境中所存储、传输和处理信息的安全需求，从五个层面的安全，明确局域计算环境的安全机制配置。

a） 物理安全

按 GB/T 20271-2006 中 6.1.1 的相关要求，在局域计算环境范围内，配置具有一级安全的下列物理安全机制：

——环境安全机制；

——设备安全机制；

——介质安全机制；

——其它物理安全机制。

b） 系统安全

按 GB/T 20272-2006 中 4.1 的要求和 GB/T 20273-2006 中 5.1 的要求，在各类计算机上配置具有下列安全机制的一级安全操作系统和数据库管理系统：

——操作系统安全性检测分析机制和数据库管理系统安全性检测分析机制；

——恶意代码防护机制；

——备份与恢复机制；

——身份鉴别机制；

——粗粒度自主访问控制机制；

——存储和传输数据完整性保护机制；

——其它系统安全机制。

c） 网络安全

按 GB/T 20270-2006 中 7.1 的要求，在局域网范围配置具有一级安全的下列安全产品和/或安全机制：

——恶意代码防护机制；

——备份与恢复机制；

——网络协议安全机制；

——存储和传输数据完整性保护机制；

——网络应用安全机制；

——其它网络安全机制。

d） 应用安全

按 GB/T 20271-2006 中 6.1.2、6.1.3、6.1.4、6.1.5 和 6.1.6 的相关要求，在应用软件系统中配置具有一级安全的下列安全机制：

——备份与故障恢复机制；

——身份鉴别机制；

——粗粒度自主访问控制机制；

——存储和传输数据完整性保护机制；

——其它应用安全机制。

4.1.3.2 二级安全机制

按 GA/T 709-2007 中图 3 所给出的具有二级安全的信息系统安全基本模型，根据局域计算环境中所存储、传输和处理信息的安全需求，从五个层面的安全，明确局域计算环境的安全机制配置。

a） 物理安全

按 GB/T 20271-2006 中 6.2.1 的相关要求，在局域计算环境范围内，配置具有二级安全的下列物理安全机制：

——环境安全机制；

——设备安全机制；

——介质安全机制；

——其它物理安全机制。

b） 系统安全

按 GB/T 20272-2006 中 4.2 的要求和 GB/T 20273-2006 中 5.2 的要求，在各类计算机上配置具有下列安全机制的二级安全操作系统和数据库管理系统：

——操作系统安全性检测分析机制和数据库管理系统安全性检测分析机制；

——安全审计机制；
——恶意代码防护机制；
——备份与故障恢复机制；
——应急处理机制；
——增强的身份鉴别机制；
——细粒度自主访问控制机制；
——存储和传输数据保密性保护机制；
——存储和传输数据完整性保护机制；
——其它系统安全机制。

c） 网络安全

按 GB/T 20270-2006 中 7.2 的要求，在局域网范围配置具有二级安全的下列安全产品和/或安全机制：

——网络安全性检测分析机制；
——安全审计机制；
——恶意代码防护机制；
——备份与故障恢复机制；
——应急处理机制；
——网络协议安全机制；
——存储和传输数据保护安全机制；
——网络应用安全机制；
——其它网络安全机制。

d） 应用安全

按 GB/T 20271-2006 中 6.2.2、6.2.3、6.2.4、6.2.5 和 6.2.6 的相关要求，在应用软件系统中配置具有二级安全的下列安全机制：

——安全性检测分析机制；
——安全审计机制；
——备份与故障恢复机制；
——应急处理机制；
——增强的身份鉴别机制；
——抗抵赖机制；
——细粒度自主访问控制机制；
——存储和传输数据保密性保护机制；
——存储和传输数据完整性保护机制；
——其它应用安全机制。

4.1.3.3 三级安全机制

按 GA/T BBBB –XXXX 中图 4 所给出的具有三级安全的信息系统安全基本模型，根据局域计算环境中所存储、传输和处理信息的安全需求，从五个层面的安全，明确局域计算环境的安全机制配置。

a） 物理安全

按 GB/T 20271-2006 中 6.3.1 的相关要求，在局域计算环境范围内，配置具有三级安全的下列物理安全机制：

——环境安全机制；
——设备安全机制；
——介质安全机制；

——其它物理安全机制。

b） 系统安全

按 GB/T 20272-2006 中 4.3 的要求和 GB/T 20273-2006 中 5.3 的要求，在各类计算机上配置具有下列安全机制的三级安全操作系统和数据库管理系统：

——操作系统安全性检测分析机制和数据库管理系统安全性检测分析机制；

——安全审计机制；

——恶意代码防护机制；

——备份与故障恢复机制；

——应急处理机制；

——身份鉴别机制；

——自主访问控制机制；

——标记与强制访问控制机制；

——存储和传输数据保密性保护（含剩余信息保护）机制；

——存储和传输数据完整性保护机制；

——其它系统安全机制。

c） 网络安全

按 GB/T 20270-2006 中 7.3 的要求，在局域网范围配置具有三级安全的下列安全产品和/或安全机制：

——网络安全性检测分析机制；

——安全审计机制；

——恶意代码防护机制；

——备份与故障恢复机制；

——应急处理机制；

——网络协议安全机制；

——存储和传输数据保护机制；

——网络应用安全机制；

——其它网络安全机制。

d） 应用安全

按 GB/T 20271-2006 中 6.3.2、6.3.3、6.3.4、6.3.5 和 6.3.6 的相关要求，在应用软件系统中配置具有三级安全的下列安全机制：

——安全性检测分析机制；

——安全审计机制；

——备份与故障恢复机制；

——应急处理机制；

——身份鉴别机制；

——抗抵赖机制；

——自主访问控制机制；

——标记与强制访问控制机制；

——存储和传输数据保密性保护机制；

——存储和传输数据完整性保护机制；

——其他应用安全机制。

4.1.3.4 四级安全机制

按 GA/T BBBB –XXXX 中图 5 所给出的具有四级安全的信息系统安全基本模型，根据局域计算

环境中所存储、传输和处理信息的安全需求，从五个层面的安全，明确局域计算环境的安全机制配置。

a) 物理安全

按 GB/T 20271-2006 中 6.4.1 的相关要求，在局域计算环境范围内，配置具有四级安全的下列物理安全机制：

——环境安全机制；

——设备安全机制；

——介质安全机制；

——其它物理安全机制。

b) 系统安全

按 GB/T 20272-2006 中 4.4 的要求和 GB/T 20273-2006 中 5.4 的要求，在各类计算机上配置具有下列安全机制的四级安全操作系统和数据库管理系统：

——操作系统安全性检测分析机制和数据库管理系统安全性检测分析机制；

——安全审计机制；

——恶意代码防护机制；

——备份与故障恢复机制；

——应急处理机制；

——身份鉴别机制；

——完全控制的自主访问控制机制；

——完全控制的标记与强制访问控制机制；

——存储和传输数据保密性保护机制；

——存储和传输数据完整性保护机制

——可信路径机制；

——其它系统安全机制。

c) 网络安全

按 GB/T 20270-2006 中 7.4 的要求，在局域网范围配置具有四级安全的下列安全产品和/或安全机制：

——网络安全性检测分析机制；

——安全审计机制；

——恶意代码防护机制；

——备份与故障恢复机制；

——应急处理机制；

——网络协议安全机制；

——存储和传输数据保护机制；

——网络应用安全机制；

——其它网络安全机制。

d) 应用安全

按 GB/T 20271-2006 中 6.4.2、6.4.3、6.4.4、6.4.5 和 6.4.6 的相关要求，在应用软件系统中配置具有四级安全的下列安全机制：

——安全性检测分析机制；

——安全审计机制；

——备份与故障恢复机制；

——应急处理机制；

——更严格的身份鉴别机制；

——抗抵赖机制；
——完全控制的自主访问控制机制；
——完全控制标记与强制访问控制机制；
——存储和传输数据保密性保护机制；
——存储和传输数据完整性保护机制；
——可信路径机制；
——其它应用软件系统安全机制。

4.1.3.5 五级安全机制

按 GA/T 709 –2007 中图 6 所给出的具有五级安全的信息系统安全基本模型，根据局域计算环境中所存储、传输和处理信息的安全需求，从五个层面的安全，明确局域计算环境的安全机制配置。

a) 物理安全

按 GB/T 20271-2006 中 6.5.1 的相关要求，在局域计算环境范围内，配置具有五级安全的下列物理安全机制：

——环境安全机制；
——设备安全机制；
——介质安全机制；
——其它物理安全机制。

b) 系统安全

按 GB/T 20272-2006 中 4.5 的要求和 GB/T 20273-2006 中 5.5 的要求，在各类计算机上配置具有下列安全机制的五级安全操作系统和数据库管理系统：

——操作系统安全性检测分析机制和数据库管理系统安全性检测分析机制；
——安全审计机制；
——恶意代码防护机制；
——备份与故障恢复机制；
——应急处理机制；
——更严格的身份鉴别机制；
——完全控制的自主访问控制机制；
——完全控制的标记与强制访问控制机制；
——存储和传输数据保密性保护机制；
——存储和传输数据完整性保护机制；
——可信路径机制；
——其它系统安全机制。

c) 网络安全

按 GB/T 20270-2006 中 7.5 的要求，在局域网范围配置具有五级安全的下列安全产品和/或安全机制：

——网络安全性检测分析机制；
——安全审计机制；
——恶意代码防护机制；
——备份与故障恢复机制；
——应急处理机制；
——网络协议安全机制；
——存储和传输数据保护机制；
——网络应用安全机制；

——其它网络安全机制。

d) 应用安全

按 GB/T 20271-2006 中 6.5.2、6.5.3、6.5.4、6.5.5 和 6.5.6 的相关要求，在应用软件系统中配置具有五级安全的下列安全机制：

——安全性检测分析机制；

——安全审计机制；

——备份与故障恢复机制；

——应急处理机制；

——身份鉴别机制；

——抗抵赖机制；

——完全控制的自主访问控制机制；

——完全控制的标记与强制访问控制机制；

——存储和传输数据保密性保护机制；

——存储和传输数据完整性保护机制；

——可信路径机制；

——其它应用软件系统安全机制。

4.2 局域计算环境边界防护及其分等级安全机制配置

4.2.1 总体要求

局域计算环境边界是指局域计算环境通过网络与外部连接的所有接口的总合。为了防止出现非定义的对外连接接口，应通过技术的或管理的手段发现并制止非法的外部接口连接（如局域网用户又通过拨号进行的外部连接等）。

局域计算环境边界防护总的目标是，按所要求的安全保护等级，通过对经边界传输的数据信息进行控制，防止来自外部的入侵和破坏，保护局域计算环境中的数据信息不被非授权的泄露和破坏，保护局域计算环境安全运行，提供有效的服务。

局域计算环境边界防护的总体要求是：

——通过对试图经边界进入的用户进行检查，防止非法用户进入本局域计算环境；

——通过对经边界输入的数据（含程序）进行检查，防止有害数据进入本局域计算环境；

——通过对经边界输出的数据进行检查，防止不该输出的数据经边界流出，防止经边界流出的数据流向较低安全保护等级的局域计算环境/独立用户或用户组；

——在实现所要求的安全保护功能的同时，提供对合法出入边界数据的应有服务。

边界防护通常由防火墙、恶意代码防护网关、入侵检测系统，以及基于密码技术的保护机制和基于信息过滤与内容控制技术的机制等共同实现或由其中的一部分机制实现，并需要实现一套完整的边界防护控制机制。

边界防护所采用的安全技术机制是与信息系统的安全性要求和所对抗攻击手段密切相关的，必须是一种与时俱进的安全措施。随着安全保护等级的提高，边界防护的安全要求分别从安全机制配置的增加、安全强度的增强和安全管理措施的加强等方面有所体现。随着信息技术和信息安全攻防技术的发展，会不断出现新的边界防护机制和产品。按 GA/T 708-2007 中 8.3.2.2 的描述，以资产价值和威胁确定的信息系统安全保护等级，是对信息系统的局域计算环境边界防护进行分等级安全机制配置的基本依据。

4.2.2 边界防护分等级安全机制配置

4.2.2.1 一级安全机制

按照 GA/T 709 –2007 中图 2 所给出的具有一级安全的信息系统安全基本模型，根据边界防护的安

全需求，按照等级保护相关技术标准的要求，明确边界防护的安全机制配置。对具有一级安全的局域计算环境的边界防护，宜配置下列安全技术机制和/或产品：

——具有一级安全的普通防火墙；

——具有一级安全的普通入侵检测机制；

——具有一级安全的普通恶意代码防护网关；

——其它具有一级安全的边界防护技术机制。

4.2.2.2 二级安全机制

按照 GA/T 709 –2007 中图 3 所给出的具有二级安全的信息系统安全基本模型，根据边界防护的安全需求，明确边界防护的安全机制配置。对具有二级安全的局域计算环境的边界防护，可配置下列安全技术机制和/或产品：

——具有二级安全的高性能防火墙；

——具有二级安全的高性能入侵检测机制；

——具有二级安全的高性能恶意代码防护网关；

——其它具有二级安全的边界防护技术机制。

4.2.2.3 三级安全机制

按照 GA/T 709 －2007 中图 4 所给出的具有三级安全的信息系统安全基本模型，根据边界防护的安全需求，按照等级保护相关技术标准的要求，明确边界防护的安全机制配置。对具有三级安全的局域计算环境的边界防护，应配置下列安全技术机制和/或产品：

——具有三级安全的高性能加固防火墙；

——具有三级安全的高性能加固入侵检测机制；

——具有三级安全的高性能加固恶意代码防护网关；

——其它具有三级安全的边界防护技术机制。

4.2.2.4 四级安全机制

按照 GA/T 709 －2007 中图 5 所给出的具有四级安全的信息系统安全基本模型，根据边界防护的安全需求，按照等级保护相关技术标准的要求，明确边界防护的安全机制配置。对具有四级安全的局域计算环境的边界防护，应配置下列安全技术机制和/或产品：

——具有四级安全的高性能加固防火墙；

——具有四级安全的高性能加固入侵检测机制；

——具有四级安全的高性能加固恶意代码防护网关；

——其它具有四级安全的边界防护技术机制。

4.2.2.5 五级安全机制

按照 GA/T 709 －2007 中图 6 所给出的具有五级安全的信息系统安全基本模型，根据边界防护的安全需求，按照等级保护相关技术标准的要求，明确边界防护的安全机制配置。对具有五级安全的局域计算环境的边界防护，应配置下列安全技术机制和/或产品：

——具有五级安全的高性能加固防火墙；

——具有五级安全的高性能加固入侵检测机制；

——具有五级安全的高性能加固恶意代码防护网关；

——其它具有五级安全的边界防护技术机制。

4.3 用户环境安全和边界防护及其分等级安全机制配置

4.3.1 总体要求

用户环境由一台或多台端计算机系统组成。根据用户环境在信息系统中所处的地位和作用，及其所存储、传输和处理的信息应保护的程度，需要对用户环境及其边界进行适当保护。用户环境及其边界防护类似于局域计算环境及其边界的保护。虽然用户环境的结构比较简单（一般只是一台个人计算

机或多台个人计算机的组合），但由于其是整个信息系统的重要组成部分，提供人对系统的操作界面，涉及信息系统安全的各方面问题，对其所进行的安全保护，需要满足信息系统整体安全要求。

用户环境安全和边界防护总的目标是，按所要求的安全保护等级，通过对端计算机系统及其边界的保护，防止来自外部的入侵和破坏，保护端计算机系统中的数据信息不被非授权的泄露和破坏，保护端计算机系统安全运行，并提供有效的服务。

用户环境安全和边界防护通常由具有相应安全等级的操作系统合数据库管理系统、端计算机系统个人防火墙、端恶意代码防护网关、入侵检测系统等安全机制实现。边界防护所采用的安全技术机制是与信息系统的安全性要求和所对抗的攻击手段密切相关的，必须是一种与时俱进的安全措施。随着安全保护等级的提高，局域计算环境边界防护的安全要求分别从安全机制配置的增加、安全强度的增强和安全管理措施的加强等方面有所体现。随着信息技术和信息安全攻防技术的发展，会不断出现新的边界防护机制和产品。按 GA/T 708-2007 中 8.3.2.2 的描述，以资产价值和威胁确定的信息系统安全保护等级，是对信息系统的用户环境安全和边界防护进行分等级安全机制配置的基本依据。

4.3.2 用户环境分等级安全机制配置

4.3.2.1 一级安全机制

按照 GA/T 709 –2007 中图 2 所给出的具有一级安全的信息系统安全基本模型，根据不同安全保护等级对端计算机系统中所存储、传输和处理的数据信息的不同安全要求，按照等级保护相关技术标准的规定，从端计算机系统保护和边界防护两方面，确定用户环境应具有的安全机制配置。对具有一级安全的用户环境的安全保护，宜配置下列安全产品和机制：

——具有一级安全的操作系统和数据库管理系统；

——具有一级安全的端计算机系统个人防火墙；

——具有一级安全的端计算机系统恶意代码防护网关；

——具有一级安全的端计算机系统入侵检测系统；

——其它具有一级安全的用户环境安全机制。

4.3.2.2 二级安全机制

按照 GA/T 709 –2007 中图 3 所给出的具有二级安全的信息系统安全基本模型，根据不同安全保护等级对终端计算机中所存储、传输和处理的数据信息的不同安全要求，按照等级保护相关技术标准的规定，从终端计算机主机保护和边界防护两方面，确定用户环境应具有的安全机制配置。对具有二级安全的用户环境的安全保护，可配置下列安全产品和机制：

——具有二级安全的操作系统和数据库管理系统；

——具有二级安全的端计算机系统个人防火墙；

——具有二级安全的端计算机系统恶意代码防护网关；

——具有二级安全的端计算机系统入侵检测系统；

——其它具有二级安全的用户环境安全机制。

4.3.2.3 三级安全机制

按照 GA/T 709 –2007 中图 4 所给出的具有三级安全的信息系统安全基本模型，根据不同安全保护等级对终端计算机中所存储、传输和处理的数据信息的不同安全要求，按照等级保护相关技术标准的规定，从终端计算机主机保护和边界防护两方面，确定用户环境应具有的安全机制配置。对具有三级安全的用户环境的安全保护，应配置下列安全产品和机制：

——具有三级安全的操作系统和数据库管理系统；

——具有三级安全的端计算机系统个人防火墙；

——具有三级安全的端计算机系统恶意代码防护网关；

——具有三级安全的端计算机系统入侵检测系统；

——其它具有三级安全的用户环境安全机制。

4.3.2.4 四级安全机制

按照 GA/T 709 –2007 中图 5 所给出的具有四级安全的信息系统安全基本模型，根据不同安全保护等级对终端计算机中所存储、传输和处理的数据信息的不同安全要求，按照等级保护相关技术标准的规定，从终端计算机主机保护和边界防护两方面，确定用户环境应具有的安全机制配置。对具有四级安全的用户环境的安全保护，应配置下列安全产品和机制：

——具有四级安全的操作系统和数据库管理系统；

——具有四级安全的端计算机系统个人防火墙；

——具有四级安全的端计算机系统恶意代码防护网关；

——具有四级安全的端计算机系统入侵检测系统；

——其它具有四级安全的用户环境安全机制。

4.3.2.5 五级安全机制

按照 GA/T 709 –2007 中图 6 所给出的具有五级安全的信息系统安全基本模型，根据不同安全保护等级对终端计算机中所存储、传输和处理的数据信息的不同安全要求，按照等级保护相关技术标准的规定，从终端计算机主机保护和边界防护两方面，确定用户环境应具有的安全机制配置。对具有五级安全的用户环境的安全保护，应配置下列安全产品和机制：

——具有五级安全的操作系统和数据库管理系统；

——具有五级安全的端计算机系统个人防火墙；

——具有五级安全的端计算机系统恶意代码防护网关；

——具有五级安全的端计算机系统入侵检测系统；

——其它具有五级安全的用户环境安全机制。

4.4 网络系统安全及其分等级安全机制配置

4.4.1 总体要求

网络系统是实现信息系统中各个局域计算环境之间或局域计算环境与用户环境之间实现相互连接的重要设施。网络系统可以是由单位或部门自行管理控制的专用网络，也可以是由各类网络服务商提供的为公众服务的互联网或虚拟专用网等网络。

网络系统安全的总体要求是，在物理安全得到保证的基础上，确保网络系统的安全运行、数据信息的安全传输及各种网络应用的安全实施。

网络系统安全运行是确保网络系统提供安全的网络服务的基础。网络系统安全运行通过采用安全性检测、安全审计、恶意代码防护、备份与故障恢复、应急计划与应急反应等措施实现。不同安全保护等级有不同的运行安全要求。

网络信息安全传输是指提供网络各个连接部分之间数据的安全传输。不同安全保护等级有不同的要求。

网络应用是指利用网络所进行的与各个业务领域相关的电子商务、电子政务、网上信息发布等网络通信与业务处理的应用，主要包括用户远程登录、Web 应用、联合计算、网络文件系统（NFS）、数据库访问、电子邮件等。网络应用安全涉及网络应用中信息的保密性、完整性、可用性以及互操作性、可控性、真实性和抗抵赖等网上数据信息的安全交换和使用。不同的安全保护等级的信息系统对网络应用有不同的安全要求。

需要指出，实现网络安全的机制和安全产品，本质上就是一个专用的信息处理系统。它们为网络系统的运行及信息在网上传输提供安全保护，其自身的安全性必须得到保证。无论是专门的网络安全装置或经过安全增强的网络设备，一方面，它们为增强网络的安全性提供了支持，另一方面，它们也增加了网络中传输数据的环节，可能引入新的脆弱性。所以，对这些网络安全产品和安全机制，同样需要按照不同安全级别的不同要求进行安全机制的自身安全保护。

随着安全保护等级的提高，网络系统的安全要求分别从安全机制配置的增加、安全强度的增强和

安全管理措施的加强等方面有所体现。按 GA/T 708-2007 中 8.3.2.2 的描述，以资产价值和威胁确定的信息系统安全保护等级，是对信息系统的网络系统进行分等级安全机制配置的基本依据。

4.4.2 网络系统分等级安全机制配置

4.4.2.1 一级安全机制

按照 GA/T 709 –2007 中图 2 所给出的具有一级安全的信息系统安全基本模型，根据不同安全保护等级对网络系统所存储、传输和处理的数据信息的不同安全需求，以及对网络系统所提供的服务的不同要求，按照等级保护相关技术标准的规定，从协议安全和数据传输整体安全出发，按物理、运行、数据传输、应用、管理等方面，确定网络系统应具有的安全机制。

a) 物理安全

按 GB/T 20271-2006 中 6.1.1 的相关要求，在网络系统范围内，配置具有一级安全的下列物理安全机制：

——环境安全机制；

——设备安全机制；

——介质安全机制；

——其它物理安全机制。

b) 运行安全

网络系统运行安全保护，宜配置下列达到一级安全要求的安全机制：

——恶意代码防护机制；

——备份与故障恢复机制；

——其它网络运行安全机制。

c) 数据传输安全

网络数据传输安全保护，宜配置下列达到一级安全要求的安全机制：

——网络协议安全机制；

——数据传输整体安全机制；

——其它数据传输安全机制。

d) 应用安全

网络应用安全保护，宜配置下列达到一级安全要求的安全机制：

——网络通信应用安全机制；

——网络信息浏览与信息管理安全机制；

——网络数据库访问与信息管理安全机制；

——网络应用自身安全保护机制；

——其它网络应用安全机制。

4.4.2.2 二级安全机制

按照 GA/T 709 –2007 中图 3 所给出的具有二级安全的信息系统安全基本模型，根据不同安全保护等级对网络系统所存储、传输和处理的数据信息的不同安全需求，以及对网络系统所提供的服务的不同要求，按照等级保护相关技术标准的规定，从协议安全和数据传输整体安全出发，按物理、运行、数据传输、应用、管理等方面，确定网络系统应具有的安全机制。

a) 物理安全

按 GB/T 20271-2006 中 6.2.1 的相关要求，在网络系统范围内，配置具有二级安全的下列物理安全机制：

——环境安全机制；

——设备安全机制；

——介质安全机制；

——其它物理安全机制。

b) 运行安全

网络系统运行安全保护，可配置下列达到二级安全要求的安全机制：

——网络安全性检测分析机制；

——安全审计机制；

——恶意代码防杀机制；

——备份与故障恢复机制；

——应急处理机制；

——其它网络运行安全机制。

c) 数据传输安全

网络数据传输安全保护，可设置下列达到二级安全要求的安全机制：

——网络协议安全机制；

——数据传输整体安全机制；

——其它数据传输安全机制。

d) 应用安全

根据网络应用的需要，进行网络应用安全保护，可配置下列达到二级安全要求的安全机制：

——网络通信应用安全机制；

——网络信息浏览与信息管理安全机制；

——网络数据库访问与信息管理安全机制；

——网络应用自身安全保护机制；

——其它网络应用安全机制。

4.4.2.3 三级安全机制

按照 GA/T 709 –2007 中图 4 所给出的具有三级安全的信息系统安全基本模型，根据不同安全保护等级对网络系统所存储、传输和处理的数据信息的不同安全需求，以及对网络系统所提供的服务的不同要求，按照等级保护相关技术标准的规定，从协议安全和数据传输整体安全出发，按物理、运行、数据传输、应用、管理等方面，确定网络系统应具有的安全机制。

a) 物理安全

按 GB/T 20271-2006 中 6.3.1 的相关要求，在网络系统范围内，配置具有三级安全的下列物理安全机制：

——环境安全机制；

——设备安全机制；

——介质安全机制；

——其它物理安全机制。

b) 运行安全

网络系统运行安全保护，应配置下列达到三级安全要求的安全机制：

——网络安全性检测分析机制；

——网络安全监控机制；

——安全审计机制；

——恶意代码防杀机制；

——备份与故障恢复机制；

——应急处理机制；

——其它网络运行安全机制。

c) 数据传输安全

网络数据传输安全保护，应配置下列达到三级安全要求的安全机制：

——网络协议安全机制；

——数据传输整体安全机制；

——其它数据传输安全机制。

d) 应用安全

网络应用安全保护，应配置下列达到三级安全要求的安全机制：

——网络通信应用安全机制；

——网络信息浏览与信息管理安全机制；

——网络数据库访问与信息管理安全机制；

——网络应用自身安全保护机制；

——其它网络应用安全机制。

4.4.2.4 四级安全机制

按照 GA/T 709 –2007 中图 5 所给出的具有四级安全的信息系统安全基本模型，根据不同安全保护等级对网络系统所存储、传输和处理的数据信息的不同安全需求，以及对网络系统所提供的服务的不同要求，按照等级保护相关技术标准的规定，从协议安全和数据传输整体安全出发，按物理、运行、数据传输、应用、管理等方面，确定网络系统应具有的安全机制。

a) 物理安全

按 GB/T 20271-2006 中 6.4.1 的相关要求，在网络系统范围内，配置具有四级安全的下列物理安全机制：

——环境安全机制；

——设备安全机制；

——介质安全机制；

——其它物理安全机制。

b) 运行安全

网络运行安全保护，应配置下列达到四级安全要求的安全机制：

——网络安全性检测分析机制；

——网络安全监控机制；

——安全审计机制；

——恶意代码防护机制；

——备份与故障恢复机制；

——应急处理机制；

——其它网络运行安全机制。

c) 传输数据安全

网络数据传输安全保护，应配置下列达到四级安全要求的安全机制：

——网络协议安全机制；

——数据传输整体安全机制；

——其它数据传输安全机制。

d) 应用安全

网络应用安全保护，应配置下列达到四级安全要求的安全机制：

——网络通信应用安全机制；

——网络信息浏览与信息管理安全机制；

——网络数据库访问与信息管理安全机制；

——网络应用自身安全保护机制；

——其它网络应用安全机制。

4.4.2.5 五级安全机制

按照 GA/T 709 –2007 中图 6 所给出的具有五级安全的信息系统安全基本模型，根据不同安全保护等级对网络系统所存储、传输和处理的数据信息的不同安全需求，以及对网络系统所提供的服务的不同要求，按照等级保护相关技术标准的规定，从协议安全和数据传输整体安全出发，按物理、运行、数据传输、应用等方面，确定网络系统应具有的安全机制。

a) 物理安全

按 GB/T 20271-2006 中 6.5.1 的相关要求，在网络系统范围内，配置具有五级安全的下列物理安全机制：

——环境安全机制；

——设备安全机制；

——介质安全机制；

——其它物理安全机制。

b) 运行安全

网络运行安全保护，应配置下列达到五级安全要求的安全机制：

——网络安全性检测分析机制；

——网络安全监控机制；

——安全审计机制；

——恶意代码防护机制；

——备份与故障恢复机制；

——应急处理机制；

——其它网络运行安全机制。

c) 数据传输安全

网络数据传输安全保护，应配置下列达到五级安全要求的安全机制：

——网络协议安全机制；

——数据传输整体安全机制；

——其它数据传输安全机制。

d) 应用安全

网络应用安全保护，应配置下列达到五级安全要求的安全机制：

——网络通信应用安全机制；

——网络信息浏览与信息管理安全机制；

——网络数据库访问与信息管理安全机制；

——网络应用自身安全保护机制；

——其它网络应用安全机制。

4.5 安全域之间互操作的安全机制配置

安全域之间互操作的安全保护包括相同安全保护等级和不同安全保护等级的局域计算环境之间互操作的安全保护，以及用户环境对局域计算环境的访问操作的安全保护。其目的是在确保应有的互操作性的同时，防止非法操作的实施，主要通过边界防护和内部访问控制来实现。其实现所需安全功能的安全机制主要包括：

——身份的鉴别机制：对试图进入本局域计算环境或登录到操作系统、数据库系统的用户的身份的真实性进行鉴别，允许注册用户进入系统；对于非注册用户，则采用代理或限制的方法，提供有限的服务，防止非法用户入侵；

——访问控制机制：通过在操作系统、数据库管理系统、应用软件系统等不同层次设置的自主访

问控制机制和强制访问控制机制，对进入系统的注册用户的访问操作进行限制，允许其对客体进行授权的访问操作，拒绝其对客体进行非授权的操作。对于非注册用户，仅提供某些约定的操作（如限定为只读等），防止其进行非法操作；

——信息流动控制机制：原则上，用户经身份鉴别和访问控制允许进入局域计算环境并登录到服务器的用户，根据其访问权限所获取的数据信息，应允许被传送到用户所在的局域计算环境、用户环境。然而，从整体上，对于由较高级别的环境向较低级别的环境流动的数据信息，需要根据总的流动规则进行整体控制。具体规则应根据实际情况确定；

——标记信息控制机制：对于在全系统范围，跨局域计算环境，按多级安全模型实施强制访问控制的主体和客体，其标记信息应在全系统范围内保持一致性。这种一致性可以用两种方法实现。一种是在跨域流动时将标记信息一起带到新的环境，另一种是在新的环境中根据整体安全要求由安全员进行重新标记；

——信息流动过程中的安全保护机制：不同等级的局域计算环境之间互操作所引起的信息流动，应按照信息在局域计算环境中的保护要求进行保护，以防止在信息流动过程中遭到泄露或破坏。比如需要较高级别保护的信息应采用加密机制进行保护等。

4.6 密码安全机制分等级配置

按照国家有关密码管理部门对密码分级管理的规定，对具有不同安全等级的信息系统，选择配置具有相应安全等级/强度的密码安全机制。按 GA/T 708-2007 中 8.3.2.2 的描述，以资产价值和威胁确定的信息系统安全保护等级，是对信息系统所用密码安全机制进行分等级配置的基本依据。

配置的密码安全机制，应从下列方面提供安全支持：

——数据存储和传输加密；

——数据存储和传输完整性检验；

——身份鉴别；

——数字签名/验证；

——网上信息交换抗抵赖等。

4.7 安全管理配置

4.7.1 安全管理总体要求及其分等级配置

4.7.1.1 总体要求

这里所说的安全管理是指与信息系统的安全技术密切相关并渗透到信息系统安全的各个组成部分的管理。通过这些安全管理措施的实施，能够使信息系统各组成部分的各种安全机制所实现的安全功能达到其应有的安全型目标。这种安全管理的总体要求是，建立一套完善的信息系统安全管理体系。通过设置必要的安全管理机制，配置必要的安全管理人员，制定必要的安全管理制度和操作规程，以及行之有效的监督、检查和责任控制，从人员管理、物理安全机制的管理、系统运行安全的管理、各种安全机制的管理以及其它与信息系统安全有关的安全管理等方面进行必要的安全管理，使管理措施落到实处。按 GA/T 708-2007 中 8.3.2.2 的描述，以资产价值和威胁确定的信息系统安全保护等级，是对信息系统的安全管理进行分等级配置的基本依据。

4.7.1.2 安全管理分等级配置

a） 一级安全管理配置

按 GB/T 20269-2006 中 6.1 和 GB/T 20271-2006 中 6.1.6 的要求，为信息系统配置具有一级安全的下列安全管理：

——人员安全管理；

——物理安全管理；

——系统运行安全管理；

——安全机制的安全管理；

——其它安全管理。

b） 二级安全管理配置

按 GB/T 20269-2006 中 6.2 和 GB/T 20271-2006 中 6.2.6 的要求，为信息系统配置具有二级安全的下列安全管理：

——人员安全管理；

——物理安全管理；

——系统运行安全管理；

——安全机制的安全管理；

——其它安全管理。

c） 三级安全管理配置

按 GB/T 20269-2006 中 6.3 和 GB/T 20271-2006 中 6.3.6 的要求，为信息系统配置具有三级安全的下列安全管理：

——人员安全管理；

——物理安全管理；

——系统运行安全管理；

——安全机制的安全管理；

——其它安全管理。

d） 四级安全管理配置

按 GB/T 20269-2006 中 6.4 和 GB/T 20271-2006 中 6.4.6 的要求，为信息系统配置具有四级安全的下列安全管理：

——人员安全管理；

——物理安全管理；

——系统运行安全管理；

——安全机制的安全管理；

——其它安全管理。

e） 五级安全管理配置

按 GB/T 20269-2006 中 6.5 和 GB/T 20271-2006 中 6.5.6 的要求，为信息系统配置具有五级安全的下列安全管理：

——人员安全管理；

——物理安全管理；

——系统运行安全管理；

——安全机制的安全管理；

——其它安全管理。

4.7.2 安全管理中心及其分等级安全机制配置

4.7.2.1 总体要求

信息系统安全管理中心的总体要求是对各种分布式控制的安全机制进行集中、统一管理，使这些安全机制充分发挥其应有的作用。除了对分布式安全机制进行集中管理外，安全管理的一个十分重要的功能是汇集各类安全机制所收集的与安全有关的信息，为系统运行中的风险分析提供一手资料。安全管理中心通过各种集中管理机制，直接或通过各个局域计算环境的分中心，实现对分布在信息系统中的各类安全机制的统一管理。一般情况下，具有三级以上安全的信息系统需要设置安全管理中心，对分布在网络环境的各个安全机制进行统一管理，对信息系统的安全进行集中控制。按 GA/T 708-2007 中 8.3.2.2 的描述，以资产价值和威胁确定的信息系统安全保护等级，是对信息系统的安全管理中心进行分等级安全机制配置的基本依据。

4.7.2.1 安全管理中心分等级安全机制配置

根据不同安全保护等级所设置的安全机制的具体情况，设置安全管理中心。安全管理中心需要从安全管理中心的物理安全以及安全管理中心的安全管理机制的设置等方面，按照不同安全保护等级的不同要求进行设计。

具有三级、四级和五级安全的信息系统，应根据系统安全机制的需要，按照 GA/T 708 –2007 中图 7 所示的信息系统安全管理中心与分布式安全机制之间关系的示意图，分别有选择地对下列安全机制进行集中管理（必要时设置安全管理分中心进行协同管理）：

——密码管理机制和 CA 系统；

——系统安全性检测、监控机制；

——恶意代码防护机制；

——用户管理机制；

——安全审计机制；

——标记管理机制；

——边界防护机制；

——其它安全机制。

参考文献

[1] GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型（idtISO/IEC 15408-1：1999）

[2] GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求（idtISO/IEC 15408-2：1999）

[3] GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求（idtISO/IEC 15408-3：1999）

[4] 信息保障技术框架（3.0版），美国国家安全局发布，国家973信息与网络安全体系研究课题组组织翻译，北京中软电子出版社，2004年4月第一版

[5] NIST SP800 , National Istitute of Standards and Technology, Technology and Ministriation,U.S.Department of Commerce