ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20271—2006

信息安全技术
信息系统通用安全技术要求

Information security technology—
Common security techniques requirement for information system

2006-05-31 发布　　2006-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准的附录A、附录B、附录C是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京思源新创信息安全资讯有限公司，江南计算技术研究所技术服务中心。

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

本标准主要从信息系统安全保护等级划分的角度，说明为实现 GB 17859—1999 中每一个安全保护等级的安全功能要求应采取的安全技术措施，以及各安全保护等级的安全功能在具体实现上的差异。

一个复杂的大型/巨大型信息系统可以由若干个分系统或子系统组成。无论从全系统、分系统或子系统的角度，信息系统一般由支持软件运行的硬件系统（含计算机硬件系统和网络硬件系统）、对系统资源进行管理和为用户使用提供基本支持的系统软件（含计算机操作系统软件、数据库管理系统软件和网络协议软件和管理软件）、实现信息系统应用功能的应用系统软件等组成。这些硬件和软件共同协作运行，实现信息系统的整体功能。从安全角度，组成信息系统各个部分的硬件和软件都应有相应的安全功能，确保在其所管辖范围内的信息安全和提供确定的服务。这些安全功能分别是：确保硬件系统安全的物理安全，确保数据网上传输、交换安全的网络安全，确保操作系统和数据库管理系统安全的系统安全（含系统安全运行和数据安全保护），确保应用软件安全运行的应用系统安全（含应用系统安全运行和数据安全保护）。这四个层面的安全，再加上为保证其安全功能达到应有的安全性而必须采取的管理措施，构成了实现信息系统安全的五个层面的安全。其实，在这五个层面中，许多安全功能和实现机制都是相同的。比如，身份鉴别、审计、访问控制、保密性保护、完整性保护等，在每一层都有体现，并有相应的安全要求。本标准对这些安全功能的描述是从安全技术的角度进行的，每一个安全技术的要求（含功能要求和保证要求）具有普遍的适用性，比如，对身份鉴别的描述既适用于操作系统，也适用于网络系统、数据库管理系统和应用系统。这种按安全要素对安全技术要求进行描述的方法，具有简洁、清晰的优点。

本标准大量采用了 GB/T 18336—2001（idt ISO/IEC 15408：1999）的安全功能要求和安全保证要求的技术内容，并按 GB 17859—1999 的五个等级，对其进行了相应的等级划分。

本标准首先对信息安全等级保护所涉及的安全功能技术要求和安全保证技术要求做了比较全面的描述，然后按 GB 17859—1999 的五个安全保护等级，对每一个安全保护等级的安全功能技术要求和安全保证技术要求做了详细描述。

需要特别说明的是，信息安全技术等级和信息系统安全等级是两个既有联系又不相同的概念。本标准是对不同安全等级的信息安全技术要求的描述。信息技术安全等级是根据安全功能技术和安全保证技术实现上的差异，参考国、内外已有标准并结合我国当前信息系统安全的实际情况确定的。而信息系统的安全等级是根据信息系统的安全需求、参照所采用的安全技术的等级确定的（有关概念的详细说明，见 A.6 关于信息安全技术等级与信息系统安全等级）。为了帮助读者运用这些安全技术设计和实现不同安全等级的信息系统，附录 B 给出了等级化信息系统安全设计参考。

附录 C 给出信息系统安全技术要素与安全技术分等级要求之间的对应关系。表 C.1 是安全功能技术要素与安全功能技术分等级要求的对应关系；表 C.2 是安全保证技术要素与安全保证技术分等级要求的对应关系。

第 6 章是对各个安全保护等级安全功能技术要求和安全保证技术要求的具体描述。为清晰表示每一个安全等级比较低一级安全等级的安全技术要求的增加和增强，每一级的新增部分用“宋体加粗字”表示。

信息安全技术
信息系统通用安全技术要求

1 范围

本标准依据 GB 17859—1999 的五个安全保护等级的划分，规定了信息系统安全所需要的安全技术的各个安全等级要求。

本标准适用于按等级化要求进行的安全信息系统的设计和实现，对按等级化要求进行的信息系统安全的测试和管理可参照使用。

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

GBJ 45—1982 高层民用建筑设计防火规定

TJ 16—1974 建筑设计防火规范

3 术语、定义和缩略语

3.1 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。

3.1.1

信息系统安全 security of information system

信息系统及其所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.1.2

信息系统通用安全技术 common security technology of information system

实现各种类型的信息系统安全所普遍适用的安全技术。

3.1.3

信息系统安全子系统 security subsystem of information system

信息系统内安全保护装置的总称，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的信息系统安全保护环境，并提供安全信息系统所要求的附加用户服务。

注：按照 GB 17859—1999 对 TCB(可信计算基)的定义，SSOIS(信息系统安全子系统)就是信息系统的 TCB。

3.1.4

安全要素 security element

本标准中的安全功能技术要求和安全保证技术要求所包含的安全内容的组成成分。

3.1.5

安全功能策略 security function policy

为实现 SSOIS 安全要素要求的功能所采用的安全策略。

3.1.6

安全功能 security function

为实现安全要素的要求，正确实施相应安全功能策略所提供的功能。