ICS 35.040
L 80

中华人民共和国国家标准

GB/T 21028—2007

信息安全技术　服务器安全技术要求

Information security technology—
Security techniques requirement for server

2007-06-29 发布　　2007-12-01 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 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。

本标准负责起草单位：浪潮电子信息产业股份有限公司。

本标准参加起草单位：联想（北京）有限公司、天津曙光计算机产业有限公司。

本标准主要起草人：孙丕恕、黄涛、孙大军、刘刚、周永利、颜斌、李清玉、景乾元、李志杰、曾宇。

引　言

本标准为设计、生产、制造、选配和使用所需要的安全等级的服务器提出了通用安全技术要求，主要从服务器安全保护等级划分的角度来说明其技术要求，即为实现 GB 17859—1999 的要求对服务器通用安全技术进行了规范。

服务器是信息系统的主要组成部分，是由硬件系统和软件系统两大部分组成的，为网络环境中的客户端计算机提供特定应用服务的计算机系统。服务器安全就是要对服务器中存储、传输、处理和发布的数据信息进行安全保护，使其免遭由于人为的和自然的原因所带来的泄漏、破坏和不可用的情况。服务器是以硬件系统和操作系统为基础，分别由数据库管理系统提供数据存储功能，以及由应用系统提供应用服务接口功能。因此，硬件系统和操作系统的安全便构成了服务器安全的基础。服务器安全从服务器组成的角度来看，硬件系统、操作系统、数据库管理系统、应用系统的安全保护构成了服务器安全。由于攻击和威胁既可能是针对服务器运行的，也可能是针对服务器中所存储、传输、处理和发布的数据信息的保密性、完整性和可用性的，所以对服务器的安全保护的功能要求，需要从系统安全运行和信息安全保护两方面综合进行考虑。本标准依据 GB/T 20271—2006 关于信息系统安全保证要素的要求，从服务器的 SSOS 自身安全保护、SSOS 的设计和实现以及 SSOS 的安全管理等方面，对服务器的安全保证要求进行更加具体的描述。

本标准按照 GB 17859—1999，分五个等级对服务器的安全功能和安全保证提出详细技术要求。其中，第 4 章对服务器安全功能基本要求进行简要说明，第 5 章从安全功能要求和安全保证要求两个方面，按硬件系统、操作系统、数据库管理系统、应用系统和运行安全五个层次对服务器安全功能的分等级要求进行了详细说明。在第 5 章的描述中除了引用前面各章的内容外，还引用了 GB/T 20271—2006 中关于安全保证技术要求的内容。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，在第 5 章的描述中，较低等级中没有出现或增强的内容用“黑体字”表示。

信息安全技术　服务器安全技术要求

1　范围

本标准依据 GB 17859—1999 的五个安全保护等级的划分，规定了服务器所需要的安全技术要求，以及每一个安全保护等级的不同安全技术要求。

本标准适用于按 GB 17859—1999 的五个安全保护等级的要求所进行的等级化服务器的设计、实现、选购和使用。按 GB 17859—1999 的五个安全保护等级的要求对服务器安全进行的测试、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在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 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

GB/T 20520—2006　信息安全技术　公钥基础设施　时间戳规范

3　术语、定义和缩略语

3.1　术语和定义

GB 17859—1999、GB/T 20271—2006、GB/T 20272—2006、GB/T 20273—2006 和 GB/T 20520—2006 确立的以及下列术语和定义适用于本标准。

3.1.1

服务器　server

服务器是信息系统的主要组成部分，是信息系统中为客户端计算机提供特定应用服务的计算机系统，由硬件系统(如处理器、存储设备、网络连接设备等)和软件系统(如操作系统、数据库管理系统、应用系统等)组成。

3.1.2

服务器安全性　server security

服务器所存储、传输、处理的信息的保密性、完整性和可用性的表征。

3.1.3

服务器安全子系统(SSOS)　security subsystem of server

服务器中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服务器安全保护环境，并提供服务器安全要求的附加用户服务。

3.1.4

安全要素　security element

本标准中各安全保护等级的安全技术要求所包含的安全内容的组成成分。