ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20279—2006

信息安全技术
网络和终端设备隔离部件安全技术要求

Information security technology—Security techniques requirements of separation components of network and terminal equipment

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：公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人：朱建平、陆臻、沈亮、邱梓华、张奕、张笑笑、顾玮、沈涛、赵婷、邹春明、顾健。

引　言

本标准是信息安全等级保护技术要求系列标准的重要组成部分，用以指导设计者如何设计和实现具有所需要的安全等级的隔离部件，主要从对隔离部件的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现基于 GB 17859—1999 的各个保护等级的安全要求对隔离部件应采取的安全技术措施，以及各安全技术要求在不同安全级中具体实现上的差异。

本标准以 GB 17859—1999 的安全等级的划分为基础，针对隔离部件的技术特点，对相应安全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。

在本标准文本中，加粗字体表示较高等级中新出现或增强的功能要求。

信息安全技术
网络和终端设备隔离部件安全技术要求

1 范围

本标准规定了对隔离部件进行安全保护等级划分所需要的详细技术要求，并给出了每一个安全保护等级的不同技术要求。

本标准适用于隔离部件的设计和实现，对隔离部件进行的测试、管理也可参照使用。

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)或修订版本均不适用于本标准，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

3 术语和定义

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

3.1

物理断开 physical disconnection

指处于不同安全域的网络之间不能以直接或间接的方式相连接。在一个物理网络环境中，实施不同安全域的网络物理断开，在技术上应确保信息在物理传导、物理存储上的断开。

3.2

协议转换 protocol conversion

在隔离部件中，协议转换的定义是协议的剥离和重建。在所属某一安全域的隔离部件一端，把基于网络的公共协议中的应用数据剥离出来，封装为系统专用协议传递至所属其他安全域的隔离部件另一端，再将专用协议剥离，并封装成需要的格式。

3.3

协议隔离 protocol separation

指处于不同安全域的网络在物理上是有连线的，通过协议转换的手段保证受保护信息在逻辑上是隔离的，只有被系统要求传输的、内容受限的信息可以通过。

3.4

信息摆渡 information ferry

信息交换的一种方式，物理传输信道只在传输进行时存在。信息传输时，信息先由信息源所在安全域一端传输至中间缓存区域，同时物理断开中间缓存区域与信息目的所在安全域的连接；随后接通中间缓存区域与信息目的所在安全域的传输信道，将信息传输至信息目的所在安全域，同时在信道上物理断开信息源所在安全域与中间缓存区域的连接。在任一时刻，中间缓存区域只与一端安全域相连。

3.5

物理断开隔离部件 physical disconnection separation components

在端上实现信息物理断开的信息安全部件，如物理隔离卡。