GB

2006年制定

中国国家标准汇编

336

GB 20279～20299

（2006 年制定）

中国标准出版社

2007

图书在版编目（CIP）数据

中国国家标准汇编：2006 年制定．336：GB 20279～20299/中国标准出版社编．—北京：中国标准出版社，2007

ISBN 978-7-5066-4500-3

Ⅰ．中… Ⅱ．中… Ⅲ．国家标准-汇编-中国-2006

Ⅳ．T-652.1

中国版本图书馆 CIP 数据核字（2007）第 060302 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码：100045
网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 47.25 字数 1 433 千字
2007 年 7 月第一版 2007 年 7 月第一次印刷

*

定价 180.00 元

ISBN 978-7-5066-4500-3

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集。自 1983 年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。本《汇编》在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2. 本《汇编》收入我国正式发布的全部国家标准。各分册中如有顺序号缺号的，除特殊情况注明外，均为作废标准号或空号。

3. 由于本《汇编》的出版时间与新国家标准的发布时间已达到基本同步，我社将在每年出版前一年发布的新制定的国家标准，便于读者及时使用。出版的形式不变，分册号继续顺延。

4. 由于标准不断修订，修订信息不能在本《汇编》中得到充分和及时的反应，根据多年来读者的要求，自 1995 年起，在本《汇编》汇集出版前一年发布的新制定的国家标准的同时，新增出版前一年发布的被修订的标准的汇编版本，视篇幅分设若干分册。这些修订标准汇编的正书名、版本形式与《中国国家标准汇编》相同，但不占总的分册号，仅在封面和书脊上注明“20××年修订-1，-2，-3，……”字样，作为本《汇编》的补充。读者配套购买则可收齐前一年制定和修订的全部国家标准。

5. 由于读者需求的变化，自第 201 分册起，仅出版精装本。

本分册为第 336 分册，收入国家标准 GB 20279～20299 的最新版本。

中国标准出版社

2007 年 4 月

目　　录

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

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。

3.6

单向隔离部件　unilateral separation components

在端上依靠硬件访问控制信息交换分区实现信息在不同的安全域信息单向流动的信息安全部件。

3.7

协议隔离部件　protocol separation components

位于两个不同安全域之间，实现协议隔离的信息安全部件。其信息流一般是专用应用数据。

3.8

网闸　gap

该信息安全部件位于两个不同安全域之间，通过协议转换的手段，以信息摆渡的方式实现数据交换，且只有被系统明确要求传输的信息可以通过。其信息流一般是通用应用服务。

4　安全环境

4.1　物理方面

对隔离部件资源的处理限定在一些可控制的访问设备内，防止未授权的物理访问。所有与实施隔离部件安全策略相关的硬件和软件应受到保护以免受未授权的物理修改。

4.2　人员方面

授权管理员不具敌意并遵守所有的管理员规则。

4.3　连通性方面

隔离部件是处于不同安全域网络之间的唯一连接点。对于物理断开隔离部件，不存在任何安全域网间的信息传输；对于单向隔离部件，信息可以从低级安全域向高级安全域通过断电非逸失性存储设备进行单向传输，反之则不能；对于协议隔离部件与网闸部件，所有安全域网络间的信息传输应经过隔离部件；授权管理员可以从高级安全域网络对隔离部件进行远程管理。

5　隔离部件分级安全技术要求

5.1　物理断开隔离部件

5.1.1　基本级要求

5.1.1.1　访问控制

5.1.1.1.1　安全属性定义

对于信息存储与传输部件(主要是处于不同安全域的存储设备、网络接入设备)，物理断开隔离部件应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.1.1.1.2　属性修改

物理断开隔离部件安全功能应向端设备用户提供修改与安全相关属性的参数的能力。

5.1.1.1.3　属性查询

物理断开隔离部件安全功能应向端设备用户提供安全属性查询的能力。

5.1.1.1.4　访问授权与拒绝

物理断开隔离部件的安全功能应对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a) 在信息物理传导上使内外网络隔断，确保外部网不能通过网络连接侵入内部网；同时阻止内部网信息通过网络连接泄露到外部网；

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部网与外部网信息要以不同存储设备分开存储；对移动存储介质，如光盘、软盘、USB 硬盘等，应在网络转换前提示用户干预或禁止在双网都能使用这些设备。

5.1.1.2 配置管理

开发者应为隔离部件产品的不同版本提供唯一的标识。

隔离部件产品的每个版本应当使用它们的唯一标识作为标签。

5.1.1.3 交付与运行

5.1.1.3.1 交付

开发者应使用一定的交付程序交付物理断开隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付物理断开隔离部件的各版本时，为维护安全所必需的所有程序。

5.1.1.3.2 安装生成

开发者应提供文档说明物理断开隔离部件的安装、生成和启动的过程。

5.1.1.4 安全功能开发过程

5.1.1.4.1 功能设计

开发者应提供隔离部件产品的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.1.1.4.2 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.1.1.5 指导性文档

5.1.1.5.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件可以使用的管理功能和接口；

b) 怎样安全地管理隔离部件；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与隔离部件的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.1.1.5.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；

b) 隔离部件提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 隔离部件安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评估而提供的其他所有文档保持一致。

5.1.1.6 测试

5.1.1.6.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的。

5.1.1.6.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.1.1.7 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.1.2 增强级要求

5.1.2.1 访问控制

5.1.2.1.1 安全属性定义

对于信息存储与传输部件(主要是处于不同安全域的存储设备、网络接入设备)，物理断开隔离部件应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.1.2.1.2 属性修改

物理断开隔离部件安全功能应向端设备用户提供修改与安全相关属性的参数的能力。

5.1.2.1.3 属性查询

物理断开隔离部件安全功能应向端设备用户提供安全属性查询的能力。

5.1.2.1.4 访问授权与拒绝

物理断开隔离部件的安全功能应对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a) 在信息物理传导上使内外网络隔断，确保外部网不能通过网络连接侵入内部网；同时阻止内部网信息通过网络连接泄露到外部网；

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部网与外部网信息要以不同存储设备分开存储；对移动存储介质，如光盘、软盘、USB 硬盘等，应在网络转换前提示用户干预或禁止在双网都能使用这些设备。

5.1.2.2 不可旁路

在与安全有关的操作(例如安全属性的修改)被允许执行之前，物理断开隔离部件安全功能应确保其通过安全功能策略的检查。

5.1.2.3 客体重用

在为所有内部或外部网上的主机连接进行资源分配时，物理断开隔离部件安全功能应保证不提供以前连接的任何信息内容。

5.1.2.4 配置管理

5.1.2.4.1 配置管理能力

开发者应使用配置管理系统并提供配置管理文档，以及为隔离部件产品的不同版本提供唯一的

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.1.2.7.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；

b) 隔离部件提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 隔离部件安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评估而提供的其他所有文档保持一致。

5.1.2.8 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.1.2.9 测试

5.1.2.9.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的，且该对应是完备的。

5.1.2.9.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

5.1.2.9.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.1.2.9.4 独立性测试

开发商应提供用于适合测试的部件，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.1.2.10 脆弱性评定

5.1.2.10.1 指南检查

开发者应提供指南性文档。

在指南性文档中，应确定对隔离部件的所有可能的操作方式(包括失败和操作失误后的操作)、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)的要求。指南性文档应是完备的、清晰的、一致的、合理的。

5.1.2.10.2 脆弱性分析

开发者应从用户可能破坏安全策略的明显途径出发，对隔离部件的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用隔离部件的环境中该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的隔离部件可以抵御明显的穿透性攻击。

5.2 单向隔离部件

5.2.1 基本级要求

5.2.1.1 访问控制

5.2.1.1.1 安全属性定义

对于信息存储与传输部件(主要是处于不同安全域的存储设备、网络接入设备)，单向隔离部件应为其设定唯一的、为了执行安全功能策略所必需的安全属性。

5.2.1.1.2 属性修改

单向隔离部件安全功能应向端设备用户提供修改与安全相关属性的参数的能力。

5.2.1.1.3 属性查询

单向隔离部件安全功能应向端设备用户提供安全属性查询的能力。

5.2.1.1.4 访问授权与拒绝

单向隔离部件的安全功能应对被隔离的计算机信息资源提供明确的访问保障能力和访问拒绝能力。在技术上确保：

a) 在信息物理传导上使内外网络隔断，确保内部网不能通过网络连接到外部网；同时保证限定外部网信息只能通过特定存储区域转移至内部网存储区域，从而阻止内部网信息通过网络连接泄露到外部网。

b) 在信息物理存储上隔断两个网络环境，对于断电后会逸失信息的部件，如内存、寄存器等暂存部件，要在网络转换时作清零处理，防止遗留信息窜网；对于断电后不会逸失信息的设备，如磁带机、硬盘等存储设备，内部网与外部网信息要分开存储并以硬件手段保证其特定的访问控制；对移动存储介质，如光盘、软盘、USB 硬盘等，应在网络转换前提示用户干预。

5.2.1.2 配置管理

开发者应为隔离部件产品的不同版本提供唯一的标识。

隔离部件产品的每个版本应当使用它们的唯一标识作为标签。

5.2.1.3 交付与运行

5.2.1.3.1 交付

开发者应使用一定的交付程序交付单向隔离部件，并将交付过程文档化。

交付文档应描述在给用户方交付单向隔离部件的各版本时，为维护安全所必需的所有程序。

5.2.1.3.2 安装生成

开发者应提供文档说明单向隔离部件的安装、生成和启动的过程。

5.2.1.4 安全功能开发过程

5.2.1.4.1 功能设计

开发者应提供隔离部件产品的安全功能设计。

功能设计应以非形式方法来描述安全功能与其外部接口，并描述使用外部安全功能接口的目的与方法，在需要的时候，还要提供例外情况和错误信息的细节。

安全功能设计应是内在一致的并能完备地表示安全功能。

5.2.1.4.2 表示对应性

开发者应在隔离部件安全功能表示的所有相邻对之间提供对应性分析。

对于隔离部件安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全

功能，应在较具体的安全功能表示中得到正确而完备地细化。

5.2.1.5 指导性文档

5.2.1.5.1 管理员指南

开发者应提供系统管理员使用的管理员指南。

管理员指南应说明以下内容：

a) 隔离部件可以使用的管理功能和接口；

b) 怎样安全地管理隔离部件；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与隔离部件的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理员有关的 IT 环境的安全要求。

管理员指南应与为评估而提供的其他所有文档保持一致。

5.2.1.5.2 用户指南

开发者应提供用户指南。

用户指南应说明以下内容：

a) 隔离部件的非管理用户可使用的安全功能和接口；

b) 隔离部件提供给用户的安全功能和接口的用法；

c) 用户可获取但应受安全处理环境控制的所有功能和权限；

d) 隔离部件安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

用户指南应与为评估而提供的其他所有文档保持一致。

5.2.1.6 测试

5.2.1.6.1 范围

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的。

5.2.1.6.2 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括测试计划、测试过程、预期的测试结果和实际测试结果。测试计划应标识要测试的安全功能，并描述测试的目标。测试过程应标识要执行的测试，并描述每个安全功能的测试概况，这些概况包括对其他测试结果的顺序依赖性。期望的测试结果应表明测试成功后的预期输出。实际测试结果应表明每个被测试的安全功能能按照规定进行运作。

5.2.1.7 生命周期支持

开发者应提供开发安全文件。

开发安全文件应描述在隔离部件的开发环境中，为保护隔离部件设计和实现的机密性和完整性，而在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在隔离部件的开发和维护过程中执行安全措施的证据。

5.2.2 增强级要求

5.2.2.1 访问控制

5.2.2.1.1 安全属性定义

对于信息存储与传输部件(主要是处于不同安全域的存储设备、网络接入设备)，单向隔离部件应为