



中华人民共和国国家标准

GB/T 20270—2006

信息安全技术 网络基础安全技术要求

Information security technology—
Basis security techniques requirement for network

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	V
引言	VI
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 网络安全组成与相互关系	2
5 网络安全功能基本要求	3
5.1 身份鉴别	3
5.1.1 用户标识	3
5.1.2 用户鉴别	3
5.1.3 用户—主体绑定	4
5.1.4 鉴别失败处理	4
5.2 自主访问控制	4
5.2.1 访问控制策略	4
5.2.2 访问控制功能	4
5.2.3 访问控制范围	4
5.2.4 访问控制粒度	4
5.3 标记	4
5.3.1 主体标记	4
5.3.2 客体标记	5
5.3.3 标记完整性	5
5.3.4 有标记信息的输出	5
5.4 强制访问控制	5
5.4.1 访问控制策略	5
5.4.2 访问控制功能	5
5.4.3 访问控制范围	6
5.4.4 访问控制粒度	6
5.4.5 访问控制环境	6
5.5 数据流控制	6
5.6 安全审计	6
5.6.1 安全审计的响应	6
5.6.2 安全审计数据产生	6
5.6.3 安全审计分析	7
5.6.4 安全审计查阅	7
5.6.5 安全审计事件选择	7
5.6.6 安全审计事件存储	7

5.7	用户数据完整性	8
5.7.1	存储数据的完整性	8
5.7.2	传输数据的完整性	8
5.7.3	处理数据的完整性	8
5.8	用户数据保密性	8
5.8.1	存储数据的保密性	8
5.8.2	传输数据的保密性	8
5.8.3	客体安全重用	8
5.9	可信路径	8
5.10	抗抵赖	8
5.10.1	抗原发抵赖	8
5.10.2	抗接收抵赖	9
5.11	网络安全监控	9
6	网络安全功能分层分级要求	9
6.1	身份鉴别功能	9
6.2	自主访问控制功能	11
6.3	标记功能	12
6.4	强制访问控制功能	13
6.5	数据流控制功能	14
6.6	安全审计功能	15
6.7	用户数据完整性保护功能	17
6.8	用户数据保密性保护功能	18
6.9	可信路径功能	20
6.10	抗抵赖功能	20
6.11	网络安全监控功能	21
7	网络安全技术分级要求	22
7.1	第一级:用户自主保护级	22
7.1.1	第一级安全功能要求	22
7.1.2	第一级安全保证要求	23
7.2	第二级:系统审计保护级	24
7.2.1	第二级安全功能要求	24
7.2.2	第二级安全保证要求	25
7.3	第三级:安全标记保护级	26
7.3.1	第三级安全功能要求	26
7.3.2	第三级安全保证要求	29
7.4	第四级:结构化保护级	30
7.4.1	第四级安全功能要求	30
7.4.2	第四级安全保证要求	33
7.5	第五级:访问验证保护级	34
7.5.1	第五级安全功能要求	34
7.5.2	第五级安全保证要求	37
附录 A (资料性附录)	标准概念说明	39
A.1	组成与相互关系	39

A.2	关于网络各层协议主要功能的说明	39
A.3	关于安全保护等级划分	40
A.4	关于主体和客体	40
A.5	关于 SSON、SSF、SSP、SFP 及其相互关系	40
A.6	关于数据流控制	41
A.7	关于密码技术	41
A.8	关于安全网络的建设	41
	参考文献	42

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、刘广明、王志强、陈冠直、景乾元、宋健平。

引 言

本标准用以指导设计者如何设计和实现具有所需要的安全保护等级的网络系统,主要说明为实现 GB 17859—1999 中每一个安全保护等级的安全要求,网络系统应采取的安全技术措施,以及各安全技术要求在不同安全保护等级中的具体差异。

网络是一个具有复杂结构、由许多网络设备组成的系统,不同的网络环境又会有不同的系统结构。然而,从网络系统所实现的功能来看,可以概括为“实现网上信息交换”。网上信息交换具体可以分解为信息的发送、信息的传输和信息的接收。从信息安全的角度,网络信息安全可以概括为“保障网上信息交换的安全”,具体表现为信息发送的安全、信息传输的安全和信息接收的安全,以及网上信息交换的抗抵赖等。网上信息交换是通过确定的网络协议实现的,不同的网络会有不同的协议。任何网络设备都是为实现确定的网络协议而设置的。典型的、具有代表性的网络协议是国际标准化组织的开放系统互连协议(ISO/OSI),也称七层协议。虽然很少有完全按照七层协议构建的网络系统,但是七层协议的理论价值和指导作用是任何网络协议所不可替代的。网络安全需要通过协议安全来实现。通过对七层协议每一层安全的描述,可以实现对网络安全的完整描述。网络协议的安全需要由组成网络系统的设备来保障。因此,对七层协议的安全要求自然包括对网络设备的安全要求。

信息安全是与信息系统所实现的功能密切相关的,网络安全也不例外。网络各层协议的安全与其在每一层所实现的功能密切相关。附录 A 中 A.2 关于网络各层协议主要功能的说明,对物理层、链路层、网络层、传输层、会话层、表示层、应用层等各层的功能进行了简要描述,是确定网络各层安全功能要求的主要依据。

本标准以 GB/T 20271—2006 关于信息系统安全等级保护的通用技术要求为基础,围绕以访问控制为核心的思想进行编写,在对网络安全的组成与相互关系进行简要说明的基础上,第 5 章对网络安全功能基本技术分别进行了说明,第 6 章是对第 5 章网络安全功能的分级分层情况的描述。在此基础上,本标准的第 7 章对网络安全技术的分等级要求分别从安全功能技术要求和安全保证技术要求两方面进行了详细说明。在第 7 章的描述中除了引用以前各章的内容外,还引用了 GB/T 20271—2006 中关于安全保证技术要求的内容。由于 GB/T 20271—2006 的安全保证技术要求,对网络而言没有需要特别说明的内容,所以在网络基本技术及其分级分层的描述中没有涉及这方面的内容。

信息安全技术

网络基础安全技术要求

1 范围

本标准依据 GB 17859—1999 的五个安全保护等级的划分,根据网络系统在信息系统中的作用,规定了各个安全等级的网络系统所需要的基础安全技术的要求。

本标准适用于按等级化的要求进行的网络系统的设计和实现,对按等级化要求进行的网络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。凡是注明日期的引用文件,其随后的所有修改单(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

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

网络安全 network security

网络环境下存储、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

网络安全基础技术 basis technology of network security

实现各种类型的网络系统安全需要的所有基础性安全技术。

3.1.3

网络安全子系统 security subsystem of network

网络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物。它建立了一个基本的网络安全保护环境,并提供安全网络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,SSON(网络安全子系统)就是网络的 TCB。

3.1.4

SSON 安全策略 SSON security policy

对 SSON 中的资源进行管理、保护和分配的一组规则。一个 SSON 中可以有一个或多个安全策略。

3.1.5

安全功能策略 security function policy

为实现 SSON 安全要素要求的功能所采用的安全策略。

3.1.6

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份。