ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18794.3—2003/ISO/IEC 10181-3:1996

信息技术　开放系统互连 开放系统安全框架 第3部分:访问控制框架

Information technology—Open Systems Interconnection—Security frameworks for open systems—Part 3:Access control framework

(ISO/IEC 10181-3:1996,Information technology—Open Systems Interconnection—Security frameworks for open systems:Access control framework,IDT)

2003-11-24 发布　　2004-08-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

目　　次

前　言

GB/T 18794《信息技术　开放系统互连　开放系统安全框架》目前包括以下几个部分：

——第 1 部分(即 GB/T 18794.1)：概述

——第 2 部分(即 GB/T 18794.2)：鉴别框架

——第 3 部分(即 GB/T 18794.3)：访问控制框架

——第 4 部分(即 GB/T 18794.4)：抗抵赖框架

——第 5 部分(即 GB/T 18794.5)：机密性框架

——第 6 部分(即 GB/T 18794.6)：完整性框架

——第 7 部分(即 GB/T 18794.7)：安全审计和报警框架

本部分为 GB/T 18794 的第 3 部分，等同采用国际标准 ISO/IEC 10181-3:1996《信息技术　开放系统互连　开放系统安全框架：访问控制框架》(英文版)。

按照 GB/T 1.1—2000 的规定，对 ISO/IEC 10181-3 作了下列编辑性修改：

a) 增加了我国的“前言”；

b) “本标准”一词改为“GB/T 18794 的本部分”或“本部分”；

c) 对“规范性引用文件”一章的导语按 GB/T 1.1—2000 的要求进行了修改；

d) 删除“规范性引用文件”一章中未被本部分引用的标准；

e) 在引用的标准中，凡已制定了我国标准的各项标准，均用我国的相应标准编号代替。对“规范性引用文件”一章中的标准，按照 GB/T 1.1—2000 的规定重新进行了排序。

本部分的附录 A 至附录 G 都是资料性附录。

本部分由中华人民共和国信息产业部提出。

本部分由中国电子技术标准化研究所归口。

本部分起草单位：四川大学信息安全研究所。

本部分主要起草人：刘嘉勇、周安民、戴宗坤、陈麟、罗万伯、屈立笳、谭兴烈。

引　言

本部分定义一个提供访问控制的通用框架。访问控制的主要目标是对抗由涉及计算机或通信系统的非授权操作所造成的威胁;这些威胁经常被细分为非授权使用、泄露、修改、破坏和拒绝服务等类别。

信息技术　开放系统互连
开放系统安全框架
第3部分:访问控制框架

1　范围

本开放系统安全框架的标准论述在开放系统环境中安全服务的应用,此处术语"开放系统"包括诸如数据库、分布式应用、开放分布式处理和开放系统互连这样一些领域。安全框架涉及定义对系统和系统内的对象提供保护的方法,以及系统间的交互。本安全框架不涉及构建系统或机制的方法学。

安全框架论述数据元素和操作的序列(而不是协议元素),这两者可被用来获得特定的安全服务。这些安全服务可应用于系统正在通信的实体,系统间交换的数据,以及系统管理的数据。

就访问控制而言,访问既可以是对一个系统(即对系统内正在通信部分的实体)的访问,也可以是对一个系统内部的访问。获取访问所要出示的信息项,以及请求该访问的顺序和该访问结果的通知都在本安全框架的考虑范围之内。不过,任何只依赖于特定应用的和严格限制在一个系统内的本地访问的信息项和操作,则不在本安全框架考虑范围之内。

许多应用要求安全措施来防止对资源的威胁,这些资源包括由开放系统互连所产生的信息。在OSI环境中,一些众所周知的威胁以及可用于防范这些威胁的安全服务和机制在GB/T 9387.2中都有所描述。

决定开放系统环境中允许使用何资源,以及在适当地方防止未授权访问的过程称作访问控制。本部分为提供访问控制服务定义通用框架。

本安全框架:

a)　定义访问控制的基本概念;

b)　示范将访问控制的基本概念具体化来支持一些公认的访问控制服务和机制的方法;

c)　定义这些服务和相应的访问控制机制;

d)　识别为支持这些访问控制服务和机制的协议的功能需求;

e)　识别为支持这些访问控制服务和机制的管理需求;

f)　阐述访问控制服务和机制与其他安全服务和机制的交互。

和其他安全服务一样,访问控制只能在为特定应用而定义的安全策略上下文内提供。访问控制策略的定义不属于本部分的范围,但本部分将会讨论到访问控制策略的一些特征。

本部分不规定提供访问控制服务可能要执行的协议交换的细节。

本部分不规定支持这些访问控制服务的具体机制,也不规定安全管理服务和协议的细节。

很多不同类型的标准能使用本框架,包括:

1)　体现访问控制概念的标准;

2)　规定含有访问控制的抽象服务的标准;

3)　规定使用访问控制服务的标准;

4)　规定在开放系统环境中提供访问控制方法的标准;

5)　规定访问控制机制的标准。

这些标准能按下列方式使用本框架:

——标准类型1)、2)、3)、4)和5)能使用本框架的术语;

——标准类型2)、3)、4)和5)能使用在本框架第7章定义的设施;