ICS 35.100.01
L 79

# 中华人民共和国国家标准

GB/T 18794.5—2003/ISO/IEC 10181-5:1996

# 信息技术　开放系统互连 开放系统安全框架 第5部分:机密性框架

**Information technology—Open Systems Interconnection—Security frameworks for open systems—Part 5:Confidentiality framework**

(ISO/IEC 10181-5:1996,Information technology—Open Systems Interconnection—Security frameworks for open systems:Confidentiality 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 5 部分，等同采用国际标准 ISO/IEC 10181-5:1996《信息技术　开放系统互连　开放系统安全框架：机密性框架》(英文版)。

按照 GB/T 1.1—2000 的规定，对 ISO/IEC 10181-5 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 E 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：戴宗坤、罗万伯、欧晓聪、龚海澎、周安民、赵勇、李焕洲。

# 引　言

许多开放系统应用都有与防止信息泄露有关的安全需求。这样的需求可能包括信息的保护，这些信息在其他安全服务如鉴别、访问控制或完整性中使用。如果这些信息被攻击者所知，就会使那些服务的效用减弱或无效。

机密性是信息对未授权个人、实体或进程不予提供或不予泄露的特性。

本部分定义提供机密性服务的通用性框架。

# 信息技术　开放系统互连
# 开放系统安全框架
# 第5部分:机密性框架

## 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。

本部分阐述在检索、传送和管理过程中信息的机密性。本部分:

1)　定义机密性的基本概念;

2)　识别可能的机密性机制类型;

3)　对每种机密性机制的设施进行分类和识别;

4)　识别用来支持各种类别的机密性机制所需的管理;

5)　阐述机密性机制和支持服务与其他安全服务和机制的交互。

许多不同类型的标准能使用这个框架,其中包括:

1)　体现机密性概念的标准;

2)　规定含有机密性的抽象服务的标准;

3)　规定使用机密性服务的标准;

4)　规定在开放系统体系结构内机密性服务的提供方法的标准;

5)　规定机密性机制的标准。

这些标准能以如下方式使用本框架:

——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)能用本框架第7章定义的设施;

——标准类型5)能基于本框架第8章定义的机制类别。

与其他的安全服务一样,机密性仅能在为一个特定应用而定义的安全策略上下文中提供。特定安全策略的定义不在本部分范围之内。

规定那些为了实现机密性所需要执行的协议交换的细节也不在本部分之内。

本部分不规定支持这些机密性服务的特殊机制,也不规定安全管理服务和协议的全部细节。支持机密性的通用机制在第8章中描述。

本安全框架中所描述的有些规程,通过应用密码技术来实现机密性。但本框架与特定的密码技术或其他算法的使用并无依赖关系,当然某些类别的机密性机制可能要依靠特殊的算法特性。

注:密码算法及其登记规程应符合我国有关规定。

本框架阐述当信息被表示成潜在攻击者可访问的数据时如何提供机密性保护。它的范围包括业务流机密性。

## 2　规范性引用文件

下述文件中的条款通过GB/T 18794的本部分的引用而成为本部分的条款。凡是注日期的引用文