ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18794.7—2003/ISO/IEC 10181-7:1996

信息技术　开放系统互连 开放系统安全框架 第7部分:安全审计和报警框架

Information technology—Open Systems Interconnection—Security frameworks for open systems—Part 7:Security audit and alarms framework

(ISO/IEC 10181-7:1996,Information technology—Open Systems Interconnection—Security frameworks for open systems: Security audit and alarms 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7部分，等同采用国际标准ISO/IEC 10181-7:1996《信息技术　开放系统互连　开放系统安全框架：安全审计和报警框架》(英文版)。

按照GB/T 1.1—2000的规定，对ISO/IEC 10181-7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) 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D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：龚海澎、周安民、李焕洲、罗万伯、戴宗坤、陈兴蜀、张力。

引　言

本部分精细化了 GB/T 18794.1 中描述的安全审计概念。它包括事件检测和从这些事件引发的动作。因此，本框架涉及安全审计和安全报警两方面。

安全审计是系统记录和活动的独立审查和检验。安全审计的目的包括：

——辅助识别和分析未经授权的动作或攻击；

——帮助确保将动作归结到为其负责的实体上；

——促进开发改进的损伤控制处理规程；

——确认符合既定的安全策略；

——报告那些可能显示系统控制缺陷的信息；

——识别可能需要的对控制、策略和处理程序的变更。

在本框架中，安全审计包括检测、收集和记录在安全审计跟踪中各种与安全有关的事件，以及分析这些事件。

审计和可确认性都要求将那些信息记录下来。安全审计保证例行事件和例外事件的足够信息均能记录下来，以便事后的调查能确定是否有违背安全的事件发生，以及如果有，则什么信息或资源受到了损害。可确认性保证将用户进行的动作或代表用户动作的处理过程的有关信息都能够记录在案，以便能将这些动作的相应后果与可疑用户(们)联系，并且能使其对自己的行为承担责任。提供安全审计服务能帮助提供可确认性。

安全报警是个人或进程发出的警告，指示发生了异常情况，可能需要马上采取动作。安全报警的目的包括：

——报告实际的或明显的安全违规企图；

——报告各种安全相关的事件，包括“正常”事件；

——报告达到一定门限而触发的事件。

信息技术　开放系统互连
开放系统安全框架
第7部分:安全审计和报警框架

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。

本部分所述安全审计和报警的目的是确保按照安全机构适当的安全策略处理与开放系统安全有关的事件。

特别是,本框架:

a)　定义安全审计和报警的基本概念;

b)　为安全审计和报警提供一个通用的模型;

c)　识别安全审计和报警服务与其他安全服务的关系。

和其他安全服务一样,安全审计只能在规定的安全策略范围内提供。

在第6章提供的安全审计和报警模型要支持很多目标,但并非所有这些目标在特定环境里都是必须的或要求的。安全审计服务为审计机构提供能力,使其能够确定需要记录在安全审计跟踪中的事件。

很多不同类型的标准能使用本框架,包括:

1)　体现审计和报警概念的标准;

2)　规定含有审计和报警的抽象服务的标准;

3)　规定使用审计和报警的标准;

4)　规定在开放系统体系结构内提供审计和报警方法的标准;

5)　规定审计和报警机制的标准。

这些标准能以下述方式使用本框架:

——标准类型1)、2)、3)和5)能使用本框架的术语;

——标准类型2)、3)、4)和5)能使用第8章定义的设施;

——标准类型5)能基于第9章定义的机制特性。

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件,其随后所有的修改单(不包括勘误的内容)或修改版均不适用于本部分,然而,鼓励根据本部分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部分。

GB/T 9387.1—1998　信息技术　开放系统互连　基本参考模型　第1部分:基本模型(idt ISO 7498-1:1989)

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)