ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 17143.8—1997
idt ISO/IEC 10164-8:1993

信息技术　开放系统互连　系统管理　第8部分：安全审计跟踪功能

Information technology—Open Systems Interconnection—Systems Management—Part 8: Security audit trail function

1997-12-15 发布　　1998-08-01 实施

国家技术监督局 发布

目　　次

前　言

本标准等同采用 ISO/IEC 10164-8:1993《信息技术　开放系统互连　系统管理:安全审计跟踪功能》和 ISO/IEC 10164-8:1993/Cor.1:1995《信息技术开放系统互连　系统管理:安全审计跟踪功能技术修改 1》。

根据 ISO/IEC 10164-8:1993/Cor.1:1995,本标准对 ISO/IEC 10164-8:1993 的第 13 章、附录 A、附录 B、附录 C、附录 D 和附录 E 进行了修改。

GB/T 17143 在《信息技术　开放系统互连　系统管理》总标题下,目前包括以下 8 个部分:

第 1 部分(即 GB/T 17143.1):客体管理功能

第 2 部分(即 GB/T 17143.2):状态管理功能

第 3 部分(即 GB/T 17143.3):表示关系的属性

第 4 部分(即 GB/T 17143.4):告警报告功能

第 5 部分(即 GB/T 17143.5):事件报告管理功能

第 6 部分(即 GB/T 17143.6):日志控制功能

第 7 部分(即 GB/T 17143.7):安全告警报告功能

第 8 部分(即 GB/T 17143.8):安全审计跟踪功能

本标准的附录 A、附录 B、附录 C、附录 D 和附录 E 是标准的附录。

本标准的附录 F 是提示的附录。

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准起草单位:电子工业部标准化研究所。

本标准主要起草人:郑洪仁、周小华、张小涛、黄家英。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(他们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC 1。由联合技术委员会提出的国际标准草案需分发给国家成员体进行表决。发布一项国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 10164-8 是由 ISO/IEC JTC 1"信息技术"联合技术委员会与 CCITT 合作制定的。等同文本为 CCITT X.740。

ISO/IEC 10164 在《信息技术　开放系统互连　系统管理》总标题下,目前包括以下 14 个部分:

——第 1 部分:客体管理功能
——第 2 部分:状态管理功能
——第 3 部分:表示关系的属性
——第 4 部分:告警报告功能
——第 5 部分:事件报告管理功能
——第 6 部分:日志控制功能
——第 7 部分:安全告警报告功能
——第 8 部分:安全审计跟踪功能
——第 9 部分:访问控制的客体和属性
——第 10 部分:记帐计量功能
——第 11 部分:工作负荷监控功能
——第 12 部分:测试管理功能
——第 13 部分:概括功能
——第 14 部分:可信度及诊断测试分类

附录 A、B、C、D 和 E 构成为本标准的一部分;附录 F 仅提供参考信息。

引　言

GB/T 17143是遵照GB 9387和GB/T 9387.4制定的由多个部分组成的标准。GB/T 17143与以下标准有关：

GB/T 16644　信息技术　开放系统互连　公共管理信息服务定义
GB/T 17142　信息技术　开放系统互连　系统管理综述
GB/T 17175　信息技术　开放系统互连　管理信息结构
GB/T 16645　信息技术　开放系统互连　公共管理信息协议

中华人民共和国国家标准

信息技术　开放系统互连　系统管理 第8部分：安全审计跟踪功能

GB/T 17143.8—1997
idt ISO/IEC 10164-8:1993

Information technology—Open Systems Interconnection—Systems Management—Part 8: Security audit trail function

1　范围

本标准定义了安全审计跟踪功能。安全审计跟踪功能是一项系统管理功能，它供应用进程在集中式或分散式管理环境中交换信息和命令，以便用于GB/T 9387.4所定义的系统管理。本标准位于GB 9387的应用层，并按GB/T 17176提供的模型定义。系统管理功能的作用由GB/T 17142描述。

本标准

——为需要用来支持安全审计跟踪报告功能的服务定义而建立用户需求；

——定义由安全审计跟踪报告功能提供的服务；

——规定为提供服务所必需的协议；

——定义服务与管理通知之间的关系；

——定义与其他系统管理功能之间的关系；

——规定一致性要求。

本标准

——不定义安全审计，也不定义如何执行安全审计。安全审计可用来帮助评估安全策略的有效性。安全策略标识要求审计的安全相关事件的分类，以及记录安全审计跟踪日志的单元；

——不定义旨在提供安全审计跟踪功能的任何实现的特性；

——不定义使用安全审计跟踪功能的适当场合；

——不定义建立、正常释放和异常释放管理联系所必需的服务；

——不定义由其他标准定义的，安全管理者可能感兴趣的任何其他通知。

2　引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB 9387—88　信息处理系统　开放系统互连　基本参考模型(idt ISO 7498:1984,eqv CCITT X.200:1988)

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/IEC 7498-2:1988,eqv CCITT X.800:1991)

GB/T 9387.4—1996　信息处理系统　开放系统互连　基本参考模型　第4部分：管理框架(idt ISO/IEC 7498-4:1989,eqv CCITT X.700:1992)

GB/T 15129—94　信息处理系统　开放系统互连　服务约定(idt ISO/TR 8509:1987,eqv CCITT X.210:1988)

国家技术监督局1997-12-15批准　　1998-08-01实施