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

GB/T 16262—1996 信息技术 开放系统互连 抽象语法记法一(ASN.1)规范(idt ISO/IEC 8824:1990,eqv CCITT X.208:1988)

GB/T 16263—1996 信息技术 开放系统互连 抽象语法记法一(ASN.1)基本编码规则规范(idt ISO/IEC 8825:1990,eqv CCITT X.209:1988)

GB/T 16644—1996 信息技术 开放系统互连 公共管理信息服务定义(idt ISO/IEC 9595:1991,eqv CCITT X.710:1991)

GB/T 17142—1997 信息技术 开放系统互连 系统管理综述(idt ISO/IEC 10040:1992)

GB/T 17143.4—1997 信息技术 开放系统互连 系统管理 第4部分:告警报告功能(idt ISO/IEC 10164-4:1992)

GB/T 17143.5—1997 信息技术 开放系统互连 系统管理 第5部分:事件报告管理功能(idt ISO/IEC 10164-5:1993)

GB/T 17143.6—1997 信息技术 开放系统互连 系统管理 第6部分:日志控制功能(idt ISO/IEC 10164-6:1993)

GB/T 17143.7—1997 信息技术 开放系统互连 系统管理 第7部分:安全告警报告功能(idt ISO/IEC 10164-7:1992)

GB/T 17175.2—1997 信息技术 开放系统互连 管理信息结构 第2部分:管理信息定义(idt ISO/IEC 10165-2:1992)

GB/T 17175.4—1997 信息技术 开放系统互连 管理信息结构 第4部分:被管客体的定义指南(idt ISO/IEC 10165-4:1992)

GB/T 17176—1997 信息技术 开放系统互连 应用层结构(idt ISO/IEC 9545:1994)

GB/T 17178.1—1997 信息技术 开放系统互连 一致性测试方法和框架 第1部分:基本概念(ISO/IEC 9646-1:1994)

ISO/IEC 9646-2:1991 信息技术 开放系统互连 一致性测试方法和框架 第2部分:抽象测试套规范

ISO/IEC 9646-7:1995 信息技术 开放系统互连 一致性测试方法和框架 第7部分:实现一致性声明

ISO/IEC 10165-6:1994 信息技术 开放系统互连 管理信息结构 第6部分:与OSI管理有关的实现一致性形式表的要求和指南

ISO/IEC 10181-7:1996 信息技术 开放系统互连 开放系统安全框架:安全审计和跟踪框架

3 定义

本标准采用下列定义。

3.1 基本参考模型定义

本标准采用GB 9387中定义的下列术语:

开放系统。

3.2 安全体系结构定义

本标准采用GB/T 9387.2中定义的下列术语:

a) 安全审计跟踪;

b) 安全策略。

3.3 管理框架定义

本标准采用GB/T 9387.4中定义的下列术语:

被管客体。

3.4 系统管理概论定义

本标准采用 GB/T 17142 中定义的下列术语：

a) 代理作用；

b) 被管客体一致性声明(MOCS)；

c) 管理信息一致性声明(MICS)；

d) 管理域；

e) 管理者作用；

f) MICS 形式表；

g) MOCS 形式表；

h) 通知；

i) 系统管理功能单元。

3.5 事件报告管理功能定义

本标准采用 GB/T 17143.1 中定义的下列术语：

辨别器。

3.6 安全告警报告定义

本标准采用 GB/T 17143.7 中定义的下列术语：

安全相关事件。

3.7 日志控制定义

本标准采用 GB/T 17143.6 中定义的下列术语：

a) 日志；

b) 日志记录。

3.8 OSI 一致性测试定义

本标准采用 GB/T 17178.1 中定义的下列术语：

a) PICS 形式表；

b) 协议实现一致性声明(PICS)；

c) 系统一致性声明。

3.9 实现一致性声明形式表定义

本标准采用 ISO/IEC 10165-6 中定义的下列术语：

a) 被管关系一致性声明(MRCS)；

b) 管理一致性概要(MCS)；

c) 管理信息定义声明(MIDS)形式表；

d) MCS 形式表；

e) MRCS 形式表。

4 缩略语

ASN.1	抽象语法记法一
CMIS	公共管理信息服务
Conf	证实
ICS	实现一致性声明
Ind	指示
MAPDU	管理应用协议数据单元
MCS	管理一致性概要
MICS	管理信息一致性声明
MIDS	管理信息定义声明

MOCS　被管客体一致性声明
MRCS　被管关系一致性声明
OSI　开放系统互连
PICS　协议实现一致性声明
Req　请求
Rsp　响应
SMAPM　系统管理应用协议机

5 约定

本标准遵循GB/T 15129定义的描述性约定为安全审计跟踪功能定义了服务。在第9章中，每项服务的定义包括一个列出服务原语参数的表。对一条给定的服务原语，每个参数的出现由下列值之一描述：

M　参数是必备的；
(=)　参数值等于左列参数之值；
U　使用该参数是服务用户的选项；
—　在该原语所描述的交互中不存在此参数；
C　参数是有条件的，条件由描述该参数的文本定义；
P　参数受GB/T 16644的强制制约。

注：在表1中标识"P"的参数，在不改变参数的语义或语法的情况下直接映射到CMIS服务原语的相应参数上。其余参数用于构造MAPDU。

6 需求

安全管理用户需要有能力在安全审计跟踪日志中记录管理域里发生的安全相关事件。开放系统的安全策略可能需要特定的安全相关事件被送给同一开放系统或不同开放系统中的安全审计跟踪日志。

可能经受安全审计制约的安全相关事件包括，但不局限于：

——连接；
——断开；
——安全机制利用；
——管理操作；
——使用记帐。

安全管理用户还需要有能力控制安全审计跟踪功能的操作。

为满足这些要求，本标准描述了这些服务和技术的用法。

7 模型

本标准要求安全相关事件按照GB/T 17143.6中定义的规程被记入日志。安全审计跟踪日志中的辨别器构造应予以规定，以便允许捕获安全策略要求记入日志的入事件。如果要将事件报告发送给不同的目的地，则应创建GB/T 17143.5中定义的事件转发辨别器，并应设置目的地址以将事件发送给选定的安全审计跟踪日志所在的系统。安全审计跟踪日志是GB/T 17143.6中定义的日志。

将事件报告运送给安全审计跟踪日志位于的系统的模型在GB/T 17143.5中定义。创建和检索安全审计跟踪日志中的项的模型在GB/T 17143.6中定义。

8 类属定义

8.1 类属通知

本标准定义一组类属安全审计跟踪通知及其可用参数和语义。

由本标准定义的这组类属通知、参数和语义集合详细提供了由 GB/T 16644 定义的 M-EVENT-REPORT 服务的下列参数：

——事件类型；

——事件信息；

——事件应答。

所有通知都是系统管理日志的潜在项。GB/T 17175.2 定义了由它派生出所有项的类属事件日志记录客体类、由事件信息规定的附加信息和事件应答参数。

8.1.1 事件类型

本参数定义安全审计跟踪报告的类型。在本标准中定义了下列事件类型：

——服务报告：指出属于拒绝或恢复服务条款的事件。生成事件的特定原因在 8.1.2 中描述；

——使用报告：指出包含与安全有关的统计特性信息的记录。

在其他标准(例如 GB/T 17143.7)中定义的其他通知可被记录在安全审计日志中。通知类型(类似于安全审计跟踪报告类型)及其有关参数在适当的标准中定义。

8.1.2 事件信息

服务报告原因参数构成通知特定事件信息。

当事件类型规定服务报告并对服务报告的可能原因定义了进一步限制时，就应提供本参数。本参数值与事件类型值一起，决定哪些参数均衡构成服务报告，以及这些参数可以是什么可能值。

用于通知，服务报告原因值应在客体类定义的行为条款中指出。本标准定义对被管客体类具有广泛适用性的服务报告原因，以在 GB/T 17142 定义的系统管理应用上下文中使用。这些值按本标准的附录 A 进行登记。服务报告原因的语法应是 ASN.1 类型客体标识符。附加的服务报告原因可被增加到本标准中，并使用在 GB/T 16262 中为 ASN.1 客体标识符值定义的登记规程登记，以在 GB/T 17142 定义的系统管理应用上下文中使用。

其他服务报告原因可以在本标准范围之外定义，并使用 GB/T 16262 中为 ASN.1 客体标识符值定义的登记规程进行登记，以在 GB/T 17142 定义的系统管理应用上下文中使用。

定义下列服务报告原因：

——请求服务：由于请求提供服务，该值规定已生成通知；

——拒绝服务：由于请求服务被拒绝，该值规定已生成通知；

——服务响应：由于请求服务被满足，该值规定已生成通知；

——服务失败：由于在提供服务的期间检测到引起服务失败的异常条件，该值规定已生成通知；

——服务恢复：由于服务已从异常条件中恢复，该值规定已生成通知；

——其他原因：由于除上述以外的原因，该值规定已生成通知。实际原因和其他相关信息在报告的其他参数中规定。

8.1.3 事件应答

该标准不规定用于事件应答参数中的管理信息。

8.2 被管客体

安全审计跟踪记录是被管客体类，它派生于在 GB/T 17175.2 中定义的事件日志记录客体类。安全审计跟踪记录客体类表示存储在由安全审计跟踪通知引起的日志中的信息。

8.3 引入的类属定义

也使用下列参数。这些参数由 GB/T 17143.4 定义：

——附加信息；

——附加文本；

——相关通知；

——通知标识符。

8.4 符合性

通过引用附录A中定义的通知样本，结合通知规范，被管客体类定义支持本标准定义的功能。引用机制在GB/T 17175.4中定义。

对每个安全审计跟踪报告的实例，都要求引入本标准定义的一个或多个安全审计跟踪通知的被管客体类定义，以便选择安全审计跟踪报告类型，使之最贴切地反映导致被管客体发出通知的真实事件。对每个引入的通知，被管客体类定义应在特性条款中规定要使用哪些选择参数和条件参数，使用它们的条件，以及它们的值。允许声明对参数的使用保留为可选。

9 服务定义

9.1 引言

安全审计跟踪通知提供报告由被管客体检测到安全相关事件的能力。本参数运送与安全审计跟踪相关的信息。

9.2 安全告警报告服务

安全告警报告服务使用第8章定义的参数，以及在GB/T 16644中定义的一般M-EVENT-REPORT服务参数。表1列出安全审计跟踪报告服务的参数。

表1 安全审计跟踪报告参数

参数名称	Req/Ind	Rsp/Conf
调用标识符	P	P
方式	P	
被管客体类	P	P
被管客体实例	P	P
事件类型	M	C(=)
事件时间	P	
事件信息		
服务报告原因	C	
通知标识符	U	
相关通知	U	
附加文本	U	
附加信息	U	
当前时间		P
事件应答		
差错		P

事件时间、相关通知和通知标识参数可由发送通知的被管客体或被管系统分配。

10 功能单元

安全审计跟踪功能构成单个系统管理功能单元。

11 协议

11.1 规程元素

11.1.1 代理作用

11.1.1.1 调用

安全审计跟踪报告规程由安全审计跟踪报告请求原语启动。在收到安全审计跟踪报告请求原语时，SMAPM 应构造一个 MAPDU，并发出一个带有参数的 CMIS M-EVENT-REPORT request 服务原语，参数来自安全审计跟踪报告请求原语。在非证实方式下，不使用 11.1.1.2 中的规程。

11.1.1.2 接收响应

在收到一个含有 MAPDU 响应安全审计跟踪报告通知的 CMIS M-EVENT-REPORT confirm 服务原语时，SMAPM 应发出一个带有参数的安全审计跟踪报告证实确认原语给安全审计跟踪报告服务用户，参数来自 CMISM-EVENT-REPORT confirm 服务原语，从而完成安全审计跟踪报告规程。

注：SMAPM 忽略收到的 MAPDU 中的所有差错。安全审计跟踪报告服务用户可以忽略这些差错，或者因此联系夭折。

11.1.2 管理者作用

11.1.2.1 接收请求

在收到一个含有 MAPDU 请求安全审计跟踪报告服务的 CMIS M-EVENT-REPORT indication 服务原语时，如果 MAPDU 完好，则 SMAPM 应发出一个带有参数的安全审计跟踪报告指示原语给安全审计跟踪报告服务用户，参数来自 CMIS M-EVENT-REPORT indication 服务原语。否则，在证实方式下，SMAPM 应构造一个含有差错通知的适当的 MAPDU，并发出一个带有差错参数存在的 CMISM-EVENT-REPORT response 服务原语。在非证实方式下，不使用 11.1.2.2 中的规程。

11.1.2.2 响应

在证实方式下，SMAPM 应接收安全审计跟踪报告响应原语，并构造一个 MAPDU 以证实通知，并发出一个带有参数的 CMIS M-EVENT-REPORT response 服务原语，参数来自安全审计跟踪报告响应原语。

11.2 抽象语法

11.2.1 被管客体

本标准定义了下列支持客体，其抽象语法在 GB/T 17175.2 中规定。

securityAuditTrailRecord

11.2.2 属性

表 2 标出了 8.1.2 中定义的参数与附录 A 中定义的属性类型规范之间的关系。

表 2 属性

参数	属性名称
服务报告原因	serviceReportCause

11.2.3 属性组

本系统管理功能没有定义属性组。

11.2.4 动作

本系统管理功能没有定义特定的动作。

11.2.5 通知

表 3 标出了 8.1.1 中定义的通知与附录 A 中定义的通知类型规范之间的关系。

表 3 通知

安全审计跟踪类型	通知类型
服务报告	serviceReport
使用报告	usageReport

MAPDU 中带有通知类型规范所引用的抽象语法。

11.2.6 服务报告原因

表 4 标出了 8.1.2 中定义的服务报告原因和附录 A 中定义的 ASN.1 值引用之间的关系。

表 4 服务报告原因

服务报告原因	ASN.1 值引用
请求服务	serviceRequest
拒绝服务	serviceDenial
服务响应	serviceResponse
服务失败	serviceFailure
服务恢复	serviceRecover
其他原因	otherReason

11.3 安全审计跟踪报告功能单元的协商

本标准分配下列客体标识符值：

{joint-iso-ccitt ms(9) function(2) part8(8) functional UnitPackage(1)}

作为在 GB/T 17142 中定义的 ASN.1 类型 FunctionalUnitPackageId 之值来协商下列功能单元：

0 security audit trail reporting functional unit

此处的数字标出了分配给功能单元的比特位置，该名称引用第 10 章中定义的功能单元。

在系统管理应用的上下文范围内，协商安全审计跟踪报告功能单元的机制由 GB/T 17142 描述。

注：协商功能单元的需求由应用上下文规定。

12 与其他功能的关系

对安全审计跟踪报告服务的控制由 GB/T 17143.5 规定的机制提供。安全审计跟踪日志属性的修改由 GB/T 17143.6 提供。

安全审计跟踪通知服务可以独立于 GB/T 17143.5 和 GB/T 17143.6 的控制服务而存在。

13 一致性

声称符合本标准的实现应遵守下列各条定义的一致性要求。

13.1 静态一致性

本实现在管理者角色、代理角色或两种角色方面应符合本标准。与至少一个角色有一致性的声称应在表 B1 中产生。

如果所产生的一致性声称是为了支持管理者角色，则该实现应支持本标准规定的至少一个通知或至少一个管理操作。这些管理操作和通知用的管理者角色的一致性要求在附录 B 引用的表 B3 和更多的表中进行标识。

如果所产生的一致性声称是为了支持代理角色，则该实现应支持本标准规定的至少一个通知。代理角色的一致性要求在附录 B 引用的表 B4 和更多的表中进行标识。

该实现应支持由 GB/T 16263 规定的名称为{joint-iso-ccitt asn1(1)basic Encoding(1)}的编码规则派生的传送语法，以便用于所声称支持的定义引用的抽象数据类型。

13.2 动态一致性

声称符合本标准的实现应支持规程元素以及与所声称支持的定义相对应的语义定义。

13.3 管理实现一致性声明要求

符合本标准的任何 MCS 形式表、MICS 形式表和 MOCS 形式表在技术上应与附录 B、C 和 D 规定的形式表相同，并保持表的编号和项的索引号，其差别仅在于页码和页头标不同。

声称符合本标准的实现供应者应完成一份在附录 B 中提供的管理一致性概要(MCS)的拷贝作为一致性要求的一部分，同时填写所引用的作为那个 MCS 可应用的任何其他 ICS 形式表。符合本标准的 ICS 应：

——描述符合本标准的实现；

——按照 ISO/IEC 10165-6 给出的填写须知将其填写好；

——包括唯一标识供应者及实现两者所必需的信息。

在别处定义的被管客体类方面，关于与本标准定义的管理信息有一致性的声称应包括被管客体类用的 MOCS 中的 MIDS 形式表要求。