ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 17143.7—1997
idt ISO/IEC 10164-7:1992

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

Information technology—Open Systems Interconnection—Systems Management—Part 7:Security alarm reporting 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 10164-7:1992《信息技术　开放系统互连　系统管理:安全告警报告功能》。

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。

ISO/IEC 10164-7 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.736。

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

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7部分：安全告警报告功能

GB/T 17143.7—1997
idt ISO/IEC 10164-7:1992

Information technology—Open Systems Interconnection—Systems Management—Part 7:Security alarm reporting function

1　范围

本标准定义了安全告警报告功能。安全告警报告功能是一项系统管理功能，它可供应用进程在集中式或分散式管理环境中交换信息，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。由本系统管理功能定义的安全告警通知提供关于操作条件和服务质量的信息，它们附属于安全。

安全相关事件与安全条款有关。每当一个安全相关事件发生时，安全策略决定要采取的行动。例如，安全策略可规定生成安全告警报告，或在安全审计跟踪时建立事件记录，或递增阈值计数器，或忽略该事件，或者采取这些行动的组合。本标准只涉及安全告警报告。

本标准

——为需要用来支持安全告警报告功能的服务定义建立用户需求；

——定义由安全告警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

——不定义旨在提供安全告警报告功能的任何实现的特性；

——不规定由安全告警报告功能的用户完成管理的方式；

——不定义任何导致使用安全告警报告功能的交互的特性；

——不规定建立、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

国家技术监督局1997-12-15批准　　1998-08-01实施

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)

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 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(idt ISO/IEC 9646-1:1994)

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) 鉴别;

b) 机密性;

c) 完整性;

d) 抗抵赖;

e) 安全策略;

f) 安全服务。

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 系统管理综述定义

本标准采用GB/T 17142中定义的下列术语:

a) 代理作用;

b) 依赖一致性；

c) 一般一致性；

d) 管理者作用；

e) 通知；

f) 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 服务约定定义

本标准采用 GB/T 15129 中定义的下列术语：

a) 服务用户；

b) 服务提供者。

3.7 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：

系统一致性声明。

3.8 补充定义

3.8.1 安全告警 security alarm

被安全策略标识为潜在违反安全的安全相关事件。

3.8.2 安全相关事件 security-related event

认为与安全有关的事件。

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
Ind	指示
MAPDU	管理应用协议数据单元
OSI	开放系统互连
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告警报告功能定义了服务。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：在本标准服务表中标明表 2 中“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

每当检测到一个指出攻击或潜在攻击系统安全的事件时，安全管理用户需要引起警觉。一个安全攻击可能被一个安全服务、一个安全机制或另一个进程检测到。

一个安全告警通知既可由任一通信端用户，也可由端用户之间的任何中间系统或进程生成。安全告警报告应如安全策略所规定的那样，标识出安全告警的原因、检测安全性相关事件的源、合适的端用户、任何误操作的被察觉的严重性、攻击或违反安全等。

为满足这些需求，本标准描述了这些服务和技术的用法。

7 模型

安全告警报告的模型在 GB/T 17143.5 中定义。信息可以根据 GB/T 17143.6 记入日志。

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的参数和语义。

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，本标准为此目的定义了被管客体类。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

本参数定义了安全告警报告的类型。本标准定义了下列事件类型：

——完整性违规：指出信息可能已被非法修改、插入或删除；

——操作违规：指出所请求的服务是不可能的，原因在于不可用性、故障或差错的服务调用；

——物理违规：暗示物理资源受到安全攻击的方式；

——安全服务或机制违规：指出安全攻击已由安全服务或机制检测到；

——时间域违规：指出一个事件发生在不期望的或禁止的时刻。

8.1.2 事件信息

下列参数构成了通知特定的事件信息。

8.1.2.1 安全告警原因

本参数为安全告警的可能原因定义了进一步的限定。本参数值与事件类型值一起，决定哪些参数均衡构成安全告警事件报告，以及这些参数可以是什么可能值。

用于通知的安全告警原因值应在客体类定义的行为条款中指出。为在 GB/T 17142 定义的系统管理应用上下文中使用，本标准定义对被管客体类具有广泛适用性的安全告警原因。这些值按 GB/T 17175.2进行登记。安全告警原因的语法应是 ASN.1 类型客体标识符。为在 GB/T 17142 中定义的系统管理应用上下文中使用，补充的安全告警原因可被增加到本标准中，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。

为在 GB/T 17142 定义的系统管理应用上下文中使用，其他安全告警原因可以在本标准范围之外定义，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。

表 1 为本标准规定的事件类型标出了安全告警原因。

表 1 安全告警原因

事件类型	安全告警原因
完整性违规	信息重复 信息失踪 检测到信息修改 信息失序 不期望的信息
操作违规	拒绝服务 停止服务 规程差错 未规定的原因
物理违规	电缆窜改 发现侵入 未规定的原因
安全服务或机制违规	鉴别失败 违反机密性 抗抵赖失败 未授权的访问企图 未规定的原因
时间域违规	延迟信息 密钥期满 违时活动

本标准定义下列安全告警原因：

——鉴别失败：指出鉴别用户的尝试不成功；

——违反机密性：指出信息可能已被未授权用户读出；

——电缆窜改：指出发生了通信媒体的物理破坏；

——延迟信息：指出收到信息比预期的晚；

——拒绝服务：指出对服务的有效请求已被阻止或不允许；

——信息重复：指出一条信息已经不止一次被收到，因此可能是重复攻击；

——信息失踪：指出未收到所期待的信息；

——检测到信息修改：指出信息已经被修改(例如由数据完整性机制指出)；

——信息失序：指出接收到的信息顺序不正确；

——发现侵入：指出标识的设备所安放的地方已被非法进入，或者设备本身已被破坏；

——密钥期满：指出有一个过时的加密钥匙已出现或已使用；

——抗抵赖失败：指出由于抗抵赖服务的失败或不可用性而阻止或停止通信；

——违时活动：指出资源利用发生在不期望的时间；

——停止服务：指出对服务的有效请求由于服务提供者的不可用性而不能得到满足；

——规程差错：指出在调用服务时，使用了一个不正确的规程；

——未授权的访问企图：指出访问控制机制已检测到访问资源的非法企图；

——不期望的信息：指出收到一个不期望的信息；

——未规定的原因：指出发生了一个未规定的、与安全有关的事件。

被管客体类定义者应选择最具体的安全告警的可用原因。

8.1.2.2 安全告警严重性

本参数定义由被管客体察觉出的安全告警的重要性。定义了下列严重性级别：

——不确定的：检测到安全攻击。尚不知道系统的完整性；

——临界的：发生了安全破坏并已危及系统。为支持安全策略，不再认为系统可正确操作。临界的严重性可能涉及未经正确的授权就修改安全信息，泄漏对系统安全至关重要的信息（诸如口令、专用加密密钥等），或破坏物理安全；

——重要的：检测到安全破坏，并已危及重要的信息或机制；

——次要的：检测到安全破坏，并已危及次要的信息或机制；

——警告：检测到安全攻击。据信尚未危及系统安全。

8.1.2.3 安全告警检测者

本参数标识安全告警的检测者。

8.1.2.4 服务用户

本参数标识其服务请求导致产生安全告警的服务用户。

8.1.2.5 服务提供者

本参数标识导致产生安全告警的服务的预期服务提供者。

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

安全告警记录是被管客体类，它派生于GB/T 17175.2中定义的事件日志记录客体类。安全告警记录客体类表示存储在由安全告警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

通过引用在GB/T 17175.2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。

对每个安全告警报告的实例，都要求引入本标准定义的一个或多个安全告警通知的被管客体类定义，以便选择安全告警类型和安全告警原因，使之最贴切地反映导致被管客体发出通知的真正事件。还要求被管客体类定义规定安全告警生成者、服务用户、服务提供者，并也应在特性条款中规定：安全告警严重性参数是如何规定的。

对每一项引入的通知，被管客体类定义应在行为条款中规定要使用哪些可选参数和条件参数、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

本标准定义一项服务。安全告警通知提供报告安全攻击、安全服务、机制误操作或其他安全相关事件的能力。本参数运送与安全告警有关的信息。

9.2 安全告警报告服务

安全告警报告服务使用本标准中第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2列出安全告警报告服务的参数。

事件时间、相关通知和通知标识符参数可由发出通知的被管客体或被管理系统分配。

表 2 安全告警报告参数

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		
安全告警原因	M	—
安全告警严重性	M	—
安全告警检测者	M	—
服务用户	M	—
服务提供者	M	—
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

10 功能单元

安全告警报告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

安全告警报告规程由安全告警报告请求原语启动。在收到安全告警报告请求原语时，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，参数来自安全告警报告请求原语。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 响应安全告警报告通知的 CMIS M-EVENT-REPORT confirm 服务原语时，SMAPM 应发出一个带有参数的安全告警报告证实原语给安全告警报告服务用户，参数来自 CMIS M-EVENT-REPORT confirm 服务原语，从而完成安全告警报告规程。

注：SMAPM 忽略收到的 MAPDU 中的所有差错。安全告警报告服务用户可以忽略这些差错，或者因此而联系夭折。

11.1.2 管理者作用

11.1.2.1 接收请求

在收到一个含有 MAPDU 请求安全告警报告服务的 CMIS M-EVENT-REPORT indication 服务原语时，如果 MAPDU 完好无损，则 SMAPM 应发出一个带有参数的安全告警报告指示原语给安全告

警报告服务用户，参数来自 CMIS M-EVENT-REPORT indication 服务原语。否则，在证实方式下，SMAPM 应构造一个适当的含有差错通知的 MAPDU，并发出一个带有差错参数存在的 CMIS M-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 应接收安全告警报告响应原语，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，参数来自安全告警报告响应原语。

11.2 抽象语法

11.2.1 被管客体

本标准引用下列支持客体，其抽象语法在 GB/T 17175.2 中规定：

securityAlarmReportRecord

11.2.2 属性

表 3 标出了本标准 8.1.2 中定义的参数与 GB/T 17175.2 中的属性类型规范之间的关系。

表 3 属性

参 数	属 性 名
安全告警原因	securityAlarmCause
安全告警严重性	securityAlarmSeverity
安全告警检测者	securityAlarmDetector
服务用户	serviceUser
服务提供者	serviceProvider

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 4 标出了本标准 8.1.1 中定义的通知与 GB/T 17175.2 中的通知类型规范之间的关系。

表 4 通知

安全告警类型	通知类型
完整性违规	integrityViolation
操作违规	operationalViolation
物理违规	physicalViolation
安全服务或机制违规	securityServiceOrMechanismViolation
时间域违规	timeDomainViolation

在 MAPDU 中携带通知类型规范所引用的抽象语法。

11.2.6 安全告警原因

表 5 标出了本标准 8.1.2.1 中定义的安全告警原因与 GB/T 17175.2 中定义的 ASN.1 参考值之间的关系。

表 5 安全告警原因

安全告警原因	ASN.1 参考值
鉴别失败	authenticationFailure
违反机密性	breachOfConfidentiality
电缆窜改	cableTamper
信息延迟	delayedInformation
拒绝服务	denialOfService
信息重复	duplicateInformation
信息失踪	informationMissing
检测到信息修改	informationModificationDetected
信息失序	informationOutOfSequence
发现侵入	intrusionDetection
密钥期满	keyExpired
抗抵赖失败	nonRepudiationFailure
违时活动	outOfHoursActivity
停止服务	outOfService
规程差错	proceduralError
未授权的访问企图	unauthorizedAccessAttempt
不期望的信息	unexpectedInformation
未规定的原因	unspecifiedReason

11.2.7 安全告警严重性值

表 6 标出了本标准 8.1.2.2 中为安全告警严重性参数定义的值与 GB/T 17175.2 中定义的 ASN.1 参考值之间的关系：

表 6 安全告警严重性值

安全告警严重性	ASN.1 值引用
不确定的	indeterminate
临界的	critical
重要的	major
次要的	minor
警告	warning

11.3 安全告警报告功能单元的协商

本标准分配下列客体标识符：

{joint-iso-ccitt ms(9)function(2)part7(7)functionalUnitPackage(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 alarm 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，协商安全告警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。