ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 29830.1—2013/ISO/IEC TR 15443-1:2005

信息技术　安全技术
信息技术安全保障框架
第1部分:综述和框架

Information technology—Security technology—A framework for IT security assurance—Part 1:Overview and framework

(ISO/IEC TR 15443-1:2005,IDT)

2013-11-12 发布　　2014-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

中 华 人 民 共 和 国
国家标准化指导性技术文件
信息技术　安全技术
信息技术安全保障框架
第 1 部分：综述和框架
GB/Z 29830.1—2013/ISO/IEC TR 15443-1:2005
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址：www.gb168.cn
服务热线：400-168-0010
010-68522006
2014 年 4 月第一版
*
书号：155066·1-48740

目　　次

前　言

GB/Z 29830《信息技术　安全技术　信息技术安全保障框架》分为以下3个部分：

——第1部分：综述和框架；

——第2部分：保障方法；

——第3部分：保障方法分析。

本部分为GB/Z 29830的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分采用翻译法等同采用ISO/IEC TR 15443-1:2005《信息技术　安全技术　信息技术安全保障框架　第1部分：综述和框架》。

本部分做了如下编辑性修改：

——国际标准2.9与2.16为重复性内容，转标时删除2.16。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分主要起草单位：中国电子技术标准化研究院。

本部分主要起草人：罗锋盈、张明天、王延鸣、陈星、杨建军。

引　言

本指导性技术文件的目的是，为了获得一个给定交付件满足其所指出的信息安全保障需求的信心，给出各种保障方法，并指导信息安全专业人员如何选择一个合适的保障方法（或组合一些方法）。这一报告审视了不同类型组织所提出的保障方法和途径，包括已批准的标准和事实标准。

为了达到这一目的，本指导性技术文件由以下7个方面内容组成：

a) 一个框架模型，用于定位现有的保障方法并给出它们之间的关系；

b) 一组保障方法以及对它们的描述和引用；

c) 特定保障方法的共性和个性的表达；

d) 现有保障方法的定性比较，其中尽可能进行定量比较；

e) 与当前保障方法关联的保障模式的标识；

f) 不同保障方法之间关系的描述；以及

g) 有关保障方法的应用、组合和认知的指导。

本指导性技术文件由3部分组成，对保障途径、分析和相互间的关系处理如下：

第1部分：综述和框架。概述了一些基础性概念，例如保障、保障框架等，并给出了安全保障方法的一般性描述。其目的是帮助理解本指导性技术文件的第2部分和第3部分内容。第1部分针对信息安全管理人员和其他人员，其中包括负责开发安全保障程序、确定他们的交付件的安全保障、参加安全评估审计或参加其他保障活动的人员。

第2部分：保障方法。描述由不同类型的组织提出和使用的各种IT安全保障方法和途径，不论它们是被一般公认的、事实上被认可的或标准的；并把这些保障方法与第1部分的保障模型关联起来。重点是识别对保障有影响的保障方法的定性特征，在可能的地方，还将定义保障级别。该材料面向IT安全专业人员，帮助理解如何在产品或服务的特定的生存周期阶段中获得保障。

GB/Z 29830.2—2013使用定义在GB/Z 29830.1—2013中的术语和定义。

该部分应与GB/Z 29830.1—2013一并使用。

第3部分：保障方法分析。分析了各种保障方法的保障特征。这个分析有助于保障机构在确定每一种保障途径的相对值并确定保障途径，使这些途径提供最适合于运行环境的具体上下文的需求的保障结果。而且，这个分析还有助于保障机构运用保障方法的结果，实现交付件所预想的确信度。这部分材料面向的对象是那些必须选择保障方法和保障途径的IT安全专业人员。

GB/Z 29830.3—2013使用定义在GB/Z 29830.1—2013中的术语和定义。

该部分应与GB/Z 29830.1—2013一并使用。

本指导性技术文件分析了一些可能不为IT安全所专有的保障方法；然而，在指导性技术文件中所给出的指导将限于IT安全需求。只对IT安全领域提供相应的指导，并不期望这一指导对一般的质量管理、评估或IT符合性具有指导意义。

信息技术　安全技术
信息技术安全保障框架
第1部分:综述和框架

1　范围

1.1　意图

GB/Z 29830 的本部分的意图是,以一种能使递增地获得交付件安全功能确信度的方式,按照一般生存周期模型,介绍交付件的安全保障方法、联系及其分类。

1.2　途径

本部分通篇采用的途径是,通过标识各种不同保障途径和保障阶段的框架,概述了一些所需要的基本概念和术语,以便理解并应用其中所涉及的保障方法。

1.3　应用

本指导性技术文件的第2部分和第3部分通过运用本部分有关保障方法的分类,指导读者针对一个给定的交付件,选择合适的保障方法以及可能的组合。

1.4　适用领域

本部分给出保障方法的分类指导,其中包括一些不是信息安全领域所特有的保障方法。在必要时,该标准可用于IT安全之外的一些领域。

1.5　限制性

本部分仅适用于交付件(参考4.3)及其相关组织信息安全问题。

2　术语和定义

下列术语和定义适用于本文件。

注:为支持本部分中的安全保障模型,给出的术语和定义尽可能具有一般性。保障模型要适用于范围宽泛的保障途径,这就要求不能把特定的术语应用于范围宽泛的保障途径。

为了满足一些可用的保障途径,已存在大量的保障术语,因此,为一个通用的保障模型定义术语是一项困难的任务。另外在现有的术语中,相似的术语具有不同的定义,并且许多术语是专为一些特定保障途径而定义的,因此为保障模型构建一个一般化的语言十分困难。面对这些困难,为了确保保障框架的固有特性,并为了适用于大量、广泛的保障方法,本指导性技术文件精心给出了术语和定义。特别地,为了保持与ISO/IEC 15408第1～3部分和ISO 9000系列标准的一致性,尽可能地采用相关的ISO标准。

接下来的一个困难是如何处理同一术语有多个定义,以及如何处理那些由于其一般性含义对保障模型不够充分而没有使用的定义。这些术语是否应予忽略或保留以便引用。如果忽略这些定义的话,在讨论中出现这些定义的保障途径时,会使读者产生困惑。如果保留特定于一种保障途径的术语,就会增加本指导性技术文件编排的复杂性;因此,本指导性技术文件在正确的上下文下来使用术语的适当定义。针对同一术语存在多个定义的情况,本指导性技术文件首先列出主要定义。可替代的定义,用半括号和斜体标出,它们仅适用于引用源的上下文。