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 29830.2—2013/ISO/IEC TR 15443-2:2005

信息技术　安全技术
信息技术安全保障框架
第2部分:保障方法

Information technology—Security technology—A framework for IT security assurance—Part 2:Assurance methods

[ISO/IEC TR 15443-2:2005,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

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2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 15443-2:2005《信息技术　安全技术　信息技术安全保障框架　第2部分：保障方法》。

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。

本部分的主要起草人：张明天、罗锋盈、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）。本指导性技术文件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标准的第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2部分:保障方法

1　范围

1.1　意图

GB/Z 29830的本部分收集了一些保障方法,其中还包括一些对整体ICT安全具有作用但不是专对ICT安全的保障方法。本部分概括了这些方法的目标,描述了它们的特征以及引用文件和标准等。

原则上,ICT安全保障的最终结果是对运行中的产品、系统或服务的保障。因此,最终的保障是应用于产品、系统或服务的生存阶段中每一种保障方法所得到的保障增量之和。大量可用的保障方法均提供了应用于一个给定领域的必要指导,以便获得公认的保障。

本部分使用GB/Z 29830.1—2013中的基本保障概念和术语,以一种概览的方式,对本部分中所收集的每一项保障方法进行分类。

通过使用这一分类,本部分指导ICT专业人员选择保障方法以及保障方法的可能组合,以适合于给定的ICT安全产品、系统或服务及其特定的环境。

1.2　适用领域

本部分以一种概括和概览的方式给出有关保障方法的指导。为了从本部分所收集的方法中获得一个量少的可用方法集合,应采用排除其中不适宜的方法这一方式从中选择之。

这一概括是描述性的,为支持分析理解原标准提供了基础。

本指导性技术文件预期读者包括:

a) 获取方(从供应方获取或取得系统、软件产品或服务的个人或组织);
b) 评价方(执行评价的个人或组织;例如,评价方可以是测试实验室、软件开发组织的一个品质部门、政府组织或用户);
c) 开发方(执行开发活动的组织或个人,包括需求分析、设计、以及软件生存周期过程期间的验收测试);
d) 维护方(执行维护活动的组织或个人);
e) 确认软件质量(授权测试)时的供应方(在获取方的合同中提供合同条款规定的系统、软件产品或软件服务的个人或组织);
f) 评估软件质量(验收测试)时的用户(使用软件产品来执行特定功能个人或组织);
g) 评估软件质量(授权测试)的安全官员或部门(对软件产品或软件服务执行系统检查的个人或部门)。

1.3　限制

本部分仅以一种综述的方式给出指导。为了更好地形成保障需求,GB/Z 29830.3提供了精化这一选择的指导,以便能够评审它们的可比较性和协作性。

支持保障途径验证并支持执行验证人员的规章制度,没有包含在本部分的范围中。