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 29830.3—2013/ISO/IEC TR 15443-3:2007

信息技术　安全技术
信息技术安全保障框架
第3部分:保障方法分析

Information technology—Security technology—A framework for IT security assurance—Part 3: Analysis of assurance methods

(ISO/IEC TR 15443-3:2007,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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
1.1　意图 …… 1
1.2　应用 …… 1
1.3　适用领域 …… 1
1.4　限制 …… 1
2　术语和定义 …… 1
3　缩略语 …… 3
4　对保障的理解 …… 4
4.1　保障目标的设置 …… 4
4.2　保障方法的应用 …… 6
4.3　保障结果的评估 …… 10
4.4　例子 …… 11
5　保障的比较、选择和组合 …… 11
5.1　保障途径的选择 …… 11
5.2　保障方法的组合 …… 13
5.3　保障方法的比较 …… 13
5.4　关注的保障特性 …… 14
6　指导 …… 18
6.1　开发保障(DA) …… 19
6.2　集成保障(IA) …… 20
6.3　运行保障(OA) …… 23
附录A(资料性附录)　列表比较 …… 26
附录B(资料性附录)　所选方法的保障特性 …… 28
附录C(资料性附录)　保障方法的组合 …… 43
参考文献 …… 45

图1　保障供给 …… 5
图2　生存周期过程管理 …… 9
图3　可用方法 …… 13
图4　矩阵比较原理 …… 14
图5　保障关注 …… 19
图6　系统测试和评价 …… 22

图 B.1　测试要求演进 …… 31

表 1　供给的保障类型 …… 5
表 2　保障供给的使用 …… 6
表 3　保障的严格程度 …… 7
表 4　保障途径应用范围 …… 7
表 5　生存周期保障模型 …… 8
表 6　保障途径 …… 10
表 7　比较的关键方面 …… 15
表 8　安全域 …… 24
表 9　安全管理特性 …… 24
表 10　整个 OA 的成熟度 …… 25
表 A.1　方法和目标用户群 …… 26
表 A.2　基本认证模式 …… 27
表 A.3　可用保障方法 …… 27

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3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 15443-3:2007《信息技术　安全技术　信息技术安全保障框架　第3部分：保障方法分析》。

本部分做了下列编辑性修改：

——国际标准中的附录D、附录E为资料性附录，转标时予以删除。

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、北京化工大学。

本部分主要起草人：王晶、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3部分:保障方法分析

1　范围

1.1　意图

GB/Z 29830的本部分的意图是:为保障机构选择合适类型的ICT(信息通信技术)保障方法提供指导,并为特定环境铺设分析特定保障方法的框架。

1.2　应用

本部分可使用户把特定保障需求和/或典型保障情况与一些可用的保障方法所提供的一般性表现特征相匹配。

1.3　适用领域

本部分的指导适用于具有安全需求的ICT产品和ICT系统的开发、实现及运行。

1.4　限制

安全需求可能是复杂的,保障方法是各式各样的,并且组织的资源和文化之间是有很大差异的。因此,本部分所给出的建议是定性的和概括性的,可能需要用户自己来分析第2部分中哪些方法最适合自己特定的交付件和组织的安全需求。

2　术语和定义

ISO/IEC TR 15443-1和ISO/IEC TR 15443-2界定的以及下列术语和定义适用于本文件。

2.1

资产　asset

对组织有价值的任何东西。

2.2

评估　assessment

系统化地检查一个实体有能力满足其规定需求的程度;当针对一个交付件时,评估是评价(evaluation)的同义词。

[ISO/IEC 14598-1]

2.3

评估方法　assessment method

为了确定一个交付件是否可以接受或发布,把特定文档化的评估准则应用于一个交付件的动作。

2.4

保障机构　assurance authority

受托对一个交付件的保障做出有关决定(即:选择、规格说明、接受、增强)的人和组织,其中,这些决