ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 17903.1—2024
代替 GB/T 17903.1—2008

信息技术　安全技术　抗抵赖
第1部分:概述

Information technology—Securitytechniques—Non-repudiation—
Part1:General

(ISO/IEC 13888-1:2020,Information security—
Non-repudiation—Part1:General,MOD)

2024-03-15发布 2024-10-01实施

国家市场监督管理总局
国家标准化管理委员会 发布

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1部分 :标准化文件的结构和起草规则》的规定起草。

本文件是 GB/T 17903《信息技术　安全技术　抗抵赖》的第 1部分。GB/T 17903 已经发布了以下部分 :

—第 1部分 :概述 ;

—第 2部分 :采用对称技术的机制 ;

—第 3部分 :采用非对称技术的机制。

本文件代替 GB/T 17903.1—2008《信息技术　安全技术　抗抵赖　第 1部分 :概述》。与 GB/T 17903.1—2008相比 ,除编辑性改动外 ,主要技术变化如下 :

a)　增加了对于杂凑函数的要求(见第 6章 ,2008版的第 6章)

b)　更改了对抗抵赖服务的表述(见 7.1、7.2,2008版的 7.1、7.2)。

本文件修改采用 ISO/IEC 13888-1:2020《信息安全　抗抵赖　第 1部分 :概述》。

本文件与 ISO/IEC 13888-1:2020的技术差异及其原因如下 :

a)　用规范性引用的 GB/T 20520替换了 ISO/IEC 18014(所有部分)(见 10.3),以适应我国的技术条件 ;

b)　增加了规范性引用的 GB/T 25069,并使用 GB/T 25069中的术语定义替代了部分原有术语的定义(见第 3章),以适应我国的技术条件 ;

c)　删除了 ISO/IEC 13888-1:2020 中第 4章的缩略语“TA”,此缩略语在正文未引用 ;

d)　删除了 ISO/IEC 13888-1:2020 中第 5章的“文档结构”,增加了“概述”,以使本文件符合国家标准的结构惯例 ;

e)　修改了对抗碰撞杂凑函数的要求(见第 6章),以适应我国的技术条件。

本文件做了下列编辑性改动 :

a)　为了与现有标准协调一致 ,将标准名称更改为《信息技术　安全技术　抗抵赖　第 1部分 :概述》;

b)　调整了术语的排列顺序 ,将按英语字母顺序排列更改为按术语间关系排列(见第 3章);

c)　用资料性引用的 GB/T 17903(所有部分)替换了 ISO/IEC 13888(所有部分)(见第 6章);

d)　删除了 ISO/IEC 13888-1:2020 中 9.1资料性引用的 ISO/IEC 14888(所有部分);

e) 用资料性引用的 GB/T 15852(所有部分)替换了 ISO/IEC9797(所有部分)(见 9.2)；