ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43577.1—2023/ISO/IEC 27050-1:2019

信息安全技术　电子发现
第1部分:概述和概念

Information security technology—Electronic discovery—Part 1:Overview and concepts

（ISO/IEC 27050-1:2019,Information technology—Electronic discovery—Part 1:Overview and concepts,IDT）

2023-12-28 发布　　2024-07-01 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 43577《信息安全技术　电子发现》的第1部分。GB/T 43577已经发布了以下部分:

——第1部分:概述和概念。

本文件等同采用ISO/IEC 27050-1:2019《信息技术　电子发现　第1部分:概述和概念》。

本文做了下列最小限度的编辑性改动:

——为与现有标准协调,将标准名称改为《信息安全技术　电子发现　第1部分:概述和概念》

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:中电长城网际系统应用有限公司、北京百度网讯科技有限公司、北京奇虎科技有限公司、国信京宁信息安全科技有限公司、北京网络行业协会电子数据司法鉴定中心、郑州信大捷安信息技术股份有限公司、国家计算机网络应急技术处理协调中心、公安部第三研究所、中国长江三峡集团有限公司、北京科软在线科技有限责任公司。

本文件主要起草人:闵京华、王海棠、张屹、郭建领、王佳慧、王笑强、杨卫军、刘为华、王文磊、舒敏、王宁、唐进、何力钊。

引　言

电子发现通常是调查以及证据获取和处理活动(ISO/IEC 27037 中涵盖)的驱动因素。此外,数据的敏感性和关键性有时候需要诸如存储安全(ISO/IEC 27040 中涵盖)之类的保护措施,以防止数据安全性受损。GB/T 43577 旨在规范电子发现的相关概念、治理与管理、过程与活动以及技术准备,拟由以下四个部分构成。

——第 1 部分:概述和概念。目的在于描述电子发现概念及其过程并定义相关术语。

——第 2 部分:电子发现的治理和管理指南。目的在于为组织高层管理人员提供电子发现的治理和管理指南。

——第 3 部分:电子发现实践指南。目的在于对电子发现过程中的各项活动提出要求和建议。

——第 4 部分:技术准备就绪。目的在于从技术和过程角度为组织规划、准备和实施电子发现提供指导。

有关 ISO/IEC 27050 的更多信息,详见第 5 章。

信息安全技术　电子发现
第1部分:概述和概念

1　范围

电子发现是指由参与调查、诉讼或类似程序的一方或多方发现相关电子留存信息(ESI)或数据的过程。本文件概述了电子发现,定义了相关术语,描述了相关概念,包括但不限于ESI的识别、保全、收集、处理、评审、分析和产出。本文件还确认了其他相关标准(如ISO/IEC 27037)及其与电子发现活动的关系和相互作用。

本文件适用于参与部分或全部电子发现活动的非技术人员和技术人员。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 27000　信息安全　安全技术　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)

注:GB/T 29246—2023　信息安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2018,IDT)

3　术语和定义

ISO/IEC 27000界定的以及下列术语和定义适用于本文件。

3.1

保管链　chain of custody

可证明的关于对材料从一个时间点到另一个时间点上的拥有、移动、处理和定位。

3.2

保管方　custodian

保管、控制或拥有电子留存信息(3.8)的个人或实体。

3.3

数据安全性受损　data breach

受保护数据的安全性降低,从而会导致其在传输、存储或其他处理过程中发生意外或非法的损毁、丢失、改动或者未授权的披露或访问。

[来源:ISO/IEC 27040:2015,3.7]

3.4

发现　discovery

一方获取另一方持有的或不被任何一方持有的与某一事项相关的信息的过程。

注1:相比对抗性纠纷中的当事方,发现的适用范围更广。

注2:发现也是指对方的硬拷贝文档、电子留存信息(3.8)和有形物品的披露。

注3:在某些司法管辖区中,术语"披露"与"发现"互换使用。