ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 47692—2026

网络安全技术　事件调查原则和过程

Cybersecurity technology—Incident investigation principles and processes

（ISO/IEC 27043:2015，Information technology—Security techniques—Incident investigation principles and processes，MOD）

2026-05-25 发布　　2026-12-01 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。

本文件修改采用ISO/IEC 27043：2015《信息技术　安全技术　事件调查原则和过程》。

本文件与ISO/IEC 27043：2015的技术差异及其原因如下：

——增加了规范性引用GB/T 25069—2022，并在“术语和定义”中使用该标准已有的定义，用规范性引用的GB/T 29246—2023替换了ISO/IEC 27000，以适应我国的技术条件；

——更改了7.13及文中其他部分的“评估结果的实施过程”为“改进过程”，以提升可读性；

——更改了8.5中“有关设备（硬件和软件）、基础设施、人员的准备”为“有关设备（硬件和软件）、策略、基础设施、人员的准备”，新增策略维度，使准备工作覆盖内容更全面；

——删除了9.4第4段“数字调查领域的专家和学者需设计出可应用于网络环境、实时调查过程、云计算环境、海量数据环境等场景的适当获取潜在数字证据的步骤”，以符合国家标准的定位；

——更改了9.5，增加“采用符合国家密码管理要求的密码”等内容，以符合我国法律要求。

本文件做了下列编辑性改动：

——更改了第1章的表述；

——对图表重新进行了编号，原因是删除了原前言，其中包括图表；

——删除了缩略语中的“DVR”，本文件中未使用该缩略语；

——更改了第5章标题“数字调查”为“数字调查原则”，以更符合本章实际内容；

——更改了5.2中针对国际差异的泛化描述，如不同司法管辖区可能存在不同法定要求，根据特定司法管辖区的特定法律、建议在特定司法管辖区内寻求法律指导等，以符合国家标准的定位；

——对6.2进行了编辑性修改，将原来各过程中逐行列出的各子过程写成一段，便于阅读，同时合并“规划事件前收集”和“事件前潜在数字证据存储和处理”，与第7章保持一致，更改“潜在数字证据存储”为“潜在数字证据存储和保全”，与第9章保持一致，在调查过程类增加“潜在数字证据获取”，与第10章保持一致；

——更改了6.2最后一段涉及数字调查过程层级结构的表述并调整至6.1第二段，以便于理解；

——在预备过程、规划过程等部分过程后面增加了“类”或“组”，表示不同层次的过程的集合，以更好地区分层次，便于理解；

——删除了7.1“上述四个目标产生的输入信息在本文件的其余部分被称为预先已知的系统输入”，后文中涉及该概念时更改了表述，以更符合中文表述习惯；

——更改了7.4中“特定管辖区的法律”为“国家法律法规要求”；

——更改了7.12中“该审查尤其需要核验是否符合特定司法体系的法律规定及数字取证原则”为“该审查尤其需要核验是否符合国家法律法规要求及数字取证原则”；

——将8.2第3段和第4段合并；

——将8.3、8.4、8.5中个别无实际意义的语句简写，并删除8.4第二段中关于数字调查预备过程类的目标相关内容，原因是7.1已经阐述，存在明显重复；

——更改了10.7中涉及不同司法管辖区的表述；

——删除了附录A（资料性附录），因该内容主要是与国际上其他数字调查模型的对比，对本文件不适用；

——为与现有网络安全国家标准协调一致，标准名称调整为《网络安全技术　事件调查原则和过程》。

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。

本文件由全国网络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:中国网络安全审查认证和市场监管大数据中心、中国电子技术标准化研究院、国家信息中心、国家工业信息安全发展研究中心、中国电子科技集团公司第十五研究所、国家信息技术安全研究中心、公安部第一研究所、司法鉴定科学研究院、亚信科技(成都)有限公司、广东中科实数科技有限公司、厦门市美亚柏科信息安全研究所有限公司、浪潮云信息技术股份公司、长扬科技(北京)股份有限公司、浪潮软件集团有限公司、杭州迪普科技股份有限公司、北京青囊风华文化传媒有限公司、杭州安恒信息技术股份有限公司。

本文件主要起草人:伍扬、田秀丽、闵京华、王惠莅、陈晨、王超佳、任欣洁、刘鑫、赵冉、王诗蕊、霍珊珊、锁延锋、刘健、马庆栋、程浩、王超杰、刘洞宾、廖双晓、郭弘、李岩、孙奕、苏步发、丁丽萍、杜漠、左鹏、饶飞、孙文龙、张增波、张亚京、刘吉林、陈星、程慧琴。

网络安全技术　事件调查原则和过程

1　范围

本文件描述了事件调查的过程和原则，包括但不限于未授权访问、数据损毁、系统崩溃或企业信息安全受损，以及其他类别的事件调查活动。

本文件适用于指导各类组织开展各种事件调查场景下涉及数字证据的调查，包括从事件前准备到调查结束的各个过程。

注：本文件不提供对每项调查活动实施原则和过程的具体描述。

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。

GB/T 25069—2022　信息安全技术　术语

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

GB/T 25069—2022、GB/T 29246—2023 界定的以及下列术语和定义适用于本文件。

3.1

获取　acquisition

〈调查取证〉在界定的集合之内创建数据副本的过程。

注：获取过程的产出是潜在数字证据的副本。

［来源：GB/T 25069—2022，3.257］

3.2

活动　activity

某一过程的内聚性任务的集合。

［来源：GB/T 25069—2022，3.256］

3.3

分析　analysis

评估潜在数字证据的过程，以评定其与事件调查的相关性。

注：潜在数字证据被确定为与事件相关时，即成为数字证据。

［来源：ISO/IEC 27042：2015，3.1］

3.4

收集　collection

对包含潜在数字证据的实体进行搜集的过程。

［来源：ISO/IEC 27037：2012，3.3］