ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 37027—2025
代替 GB/T 37027—2018

网络安全技术
网络攻击和网络攻击事件判定准则

Cybersecurity technology—Criteria for determing network attack and network attack incident

2025-02-28 发布　　2025-09-01 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。

本文件代替GB/T 37027—2018《信息安全技术　网络攻击定义及描述规范》，与GB/T 37027—2018相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了网络攻击的定义（见3.1，2018年版的3.1）；

b) 增加了网络攻击事件的定义（见3.2）；

c) 更改了“网络攻击”中“攻击技术手段”“安全漏洞类型”的描述（见5.1，2018年版的6.2、6.3）；

d) 增加了网络攻击事件的信息描述（见5.2）；

e) 增加了网络攻击的判定条件（见6.2）；

f) 增加了网络攻击事件的判定条件（见6.3）；

g) 增加了网络攻击的计数方法（见7.2）；

h) 增加了网络攻击事件的计数方法（见7.3）。

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：国家计算机网络应急技术处理协调中心、国家计算机网络应急技术处理协调中心北京分中心、中国电子技术标准化研究院、中国移动通信集团有限公司、启明星辰信息技术集团股份有限公司、安天科技集团股份有限公司、北京长亭科技有限公司、国家工业信息安全发展研究中心、国能数智科技开发（北京）有限公司、郑州信大捷安信息技术股份有限公司、北京天融信网络安全技术有限公司、国家信息中心（国家电子政务外网管理中心）、中国信息通信研究院、广东省信息安全测评中心、中科信息安全共性技术国家工程研究中心有限公司、杭州安恒信息技术股份有限公司、北京升鑫网络科技有限公司、奇安信科技集团股份有限公司、中国电子信息产业集团有限公司第六研究所、北京时代新威信息技术有限公司、江苏君立华域信息安全技术股份有限公司、北京中测安华科技有限公司、中电科网络安全科技股份有限公司、北京神州绿盟科技有限公司、三六零数字安全科技集团有限公司、杭州迪普科技股份有限公司、公安部第三研究所、国家计算机网络应急技术处理协调中心黑龙江分中心、长安通信科技有限责任公司。

本文件主要起草人：严寒冰、饶毓、郭晶、陈亮、赵彦、周莹莹、卢卫、徐剑、吕志泉、韩志辉、温森浩、王惠莅、朱雪峰、徐雅丽、李一鸣、邱勤、杨天识、刘佳男、杨坤、张晓菲、牛月坤、刘为华、安高峰、闫桂勋、董航、甄茁、胡建勋、陈彦羽、卞建超、刘勇、赵云龙、王连强 、金建军、严默默、曹旭博、肖岩军、耿贵宁、刘吉林、陶源、刘琨、张洛什。

本文件及其所代替文件的历次版本发布情况为：

——2018年首次发布为GB/T 37027—2018；

——本次为第一次修订。

引　言

近年来，随着网络应用的普及和迅猛发展，网络攻击的方法和形式复杂与多变，对网络安全造成了严重威胁。

网络攻击和网络攻击事件的判定涉及多方面因素，包括：网络攻击和网络攻击事件的区别；网络攻击和网络攻击事件的界定和分类；网络攻击及网络攻击事件涉及的角色、过程、关键技术、后果评估；各类网络攻击的和网络攻击事件的判定及计数方法等内容。随着网络攻击和网络攻击事件的日益增多，当前各组织对网络攻击、网络攻击事件判定和计数方法不统一，导致各组织判定和统计网络攻击出现较大差异，难以有效实现网络攻击态势的共享和准确感知。因此，需对网络攻击和网络攻击事件进行更加准确的定义、描述，给出统一分类、判定及统计准则，为抵御网络攻击夯实基础，提升网络攻击态势的感知效果，增强网络安全保障能力。

网络安全技术
网络攻击和网络攻击事件判定准则

1 范围

本文件确立了网络攻击和网络攻击事件的描述信息要素、判定和计数的方法。

本文件适用于指导组织开展网络攻击和网络攻击事件的监测分析、态势感知、信息报送等活动。

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 20986—2023 信息安全技术 网络安全事件分类分级指南

GB/T 30279—2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

GB/T 20986—2023、GB/T 30279—2020 界定的以及下列术语和定义适用于本文件。

3.1

网络攻击 network attack

通过信息网络技术和各种手段，利用网络中存在的安全漏洞和安全缺陷针对网络实施干扰、控制、破坏等影响网络正常运行状态，以及针对网络数据实施窃取、滥用、篡改、损毁等危害数据安全的行为。

3.2

网络攻击事件 network attack incident

网络攻击（3.1）造成或潜在造成业务损失或危害的安全事件。

4 缩略语

下列缩略语适用于本文件。

APT：高级可持续威胁攻击（advanced persistent threat）

ARP：地址解析协议（address resolution protocol）

AS：自治系统（autonomous system）

BGP：边界网关协议（border gateway protocol）

DNS：域名系统（domain name system）

HTTP：超文本传输协议（hypertext transfer protocol）

IOC：失陷指标（indicators of compromise）

IP：互联网协议（internet protocol）

WLAN：无限局域网（wireless local area network）