ICS 35.040
L 80

中华人民共和国国家标准

GB/T 38645—2020

信息安全技术　网络安全事件应急演练指南

Information security techniques—Guide for cybersecurity incident emergency exercises

2020-04-28 发布　　2020-11-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:烽台科技(北京)有限公司、国家工业信息安全发展研究中心、国家电网有限公司、国家信息技术安全研究中心、中国证监会信息中心、中国电力科学研究院有限公司、中国电子技术标准化研究院、黑龙江省工业和信息化厅、清华大学、北京京航计算通讯研究所、北京理工大学、哈尔滨工业大学、哈尔滨工程大学、桂林电子科技大学、公安部第三研究所、中国信息安全测评中心、国家计算机网络应急技术处理协调中心、中国互联网络信息中心、中国科学院信息工程研究所、中国电子科技网络信息安全有限公司、黑龙江省电子技术研究所、北京启明星辰信息安全技术有限公司、哈尔滨工大天创电子有限公司、国网山东省电力公司电力科学研究院、北京安天网络安全技术有限公司、北京网藤科技有限公司、哈尔滨工业大学软件工程股份有限公司、黑龙江信息技术职业学院、北京市政务信息安全应急处置中心、北京网御星云信息技术有限公司、北京卓识网安技术股份有限公司。

本标准主要起草人:龚亮华、尹丽波、王磊、宫亚峰、刘莹、王东明、张格、刘迎、朱朝阳、魏钦志、周亮、李琳、张永静、张洪、李俊、于盟、王达、薛一波、祝烈煌、王佰伶、孙建国、丁勇、佟薇薇、孙立立、王启蒙、雷承霖、赵旭东、邱梓华、邹春明、贾若伦、訾立强、谢丰、杜红亮、何能强、李若愚、郝志宇、敖佳、刘慧晶、郑显生、孟雅辉、刘文跃、王文婷、李柏松、童志明、李佐民、郭宇亮、左晓英、范士喜、张涛、魏彬、杜君、刘健帅、刘韧。

引　言

建立网络安全事件应急工作机制，开展应急演练是减少和预防网络安全事件造成损失和危害的重要保证。为规范和指导网络安全事件应急演练工作，制定网络安全事件应急演练指南是必要的。

信息安全技术　网络安全事件应急演练指南

1　范围

本标准给出了网络安全事件应急演练实施的目的、原则、形式、方法及规划，并描述了应急演练的组织架构以及实施过程。

本标准适用于指导相关组织实施网络安全事件应急演练活动。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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　信息安全技术　术语

3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

网络安全事件　cybersecurity incident

由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

3.2

网络安全事件应急演练　cybersecurity incident emergency exercises

有关政府部门、企事业单位、社会团体组织相关人员，针对设定的突发事件模拟情景，按照应急预案所规定的职责和程序，在特定的时间和地域，开展应急处置的活动。

4　应急演练目的

应急演练目的如下：

a) 检验预案：通过开展应急演练，查找和验证应急预案中存在的问题，完善应急预案，提高应急预案的科学性、实用性和可操作性；

b) 完善准备：通过开展应急演练，检查应对网络安全事件所需应急队伍、物资、装备、技术等方面的准备情况，发现不足及时予以调整补充，做好应急准备工作；

c) 锻炼队伍：通过开展应急演练，增强演练管理部门、指挥机构、参演机构和人员等对应急预案的熟悉程度，锻炼应急处置需要的技能，加强配合，提高其应急处置能力；

d) 磨合机制：通过开展应急演练，进一步明确相关单位和人员的职责任务，理顺工作关系，完善各关联方之间分离、阻隔、配套应急联动机制，防范网络安全风险传导；

e) 宣传教育：通过开展应急演练，普及应急知识，不断增强网络安全管理的专业化程度，提高全员网络安全风险防范意识。