ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1717.1—2020

信息安全技术　网络安全事件通报预警 第1部分:术语

Information security technology—Notification and warning of cyber security incidents—Part 1:Terminology

2020-03-24 发布　　2020-08-01 实施

中华人民共和国公安部　　发布

目　　次

前　言

GA/T 1717《信息安全技术　网络安全事件通报预警》分为三个部分：

——第1部分：术语；

——第2部分：通报预警流程规范；

——第3部分：数据分类编码与标记标签系统技术规范。

本部分为GA/T 1717的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分由公安部网络安全保卫局提出。

本部分由公安部信息系统安全标准化技术委员会归口。

本部分起草单位：公安部网络安全保卫局、公安部第三研究所、中国科学院软件研究所、太极计算机股份有限公司、启明星辰信息技术集团股份有限公司、奇安信科技集团股份有限公司、国网网安(北京)科技有限公司。

本部分主要起草人：杜佳颖、黄小苏、张秀东、吴辰苗、任彬、陈长松、高琪、张超、侯茂强、马闽、李姝、殷倩、李祉岐。

引　言

当前，网络安全形势日趋严峻、安全威胁日趋多样化、漏洞隐患频发多发、安全事件影响日趋深远，严重危害国家安全、公共安全和民众利益。

网络安全事件通报预警是国家网络安全保障体系的重要环节，是国家法律法规要求的重要工作内容。为进一步明确网络安全事件通报预警的规范化描述语言体系、工作流程规范、分类编码方法和标记标签体系，从而规范网络安全事件通报预警工作，切实维护国家关键信息基础设施安全，保障民众利益、公共安全和国家安全，特制定 GA/T 1717。

GA/T 1717 分为三部分，可为网络安全职能部门开展网络安全监测分析、通报预警、应急处置工作提供依据和参考。第 1 部分明确了网络安全事件通报预警工作中重点需要的用语及其含义，统一规范了通报预警工作各方的交互语言；第 2 部分规范了网络安全事件定级方法、通报流程和预警流程，可有效提高通报预警工作效率；第 3 部分规范了网络安全事件通报预警工作中相关数据的分类方法、编码方法和标记标签体系，可为网络安全通报预警工作的机器化、智能化、数字化开展提供支撑。

信息安全技术　网络安全事件通报预警
第1部分：术语

1　范围

GA/T 1717的本部分规定了网络安全事件通报预警所涉及的术语及其定义。

本部分适用于网络安全事件监测分析、通报预警、调查处置及相关管理和技术研究工作，准确理解和表达相关概念。

2　一般概念

2.1

攻击者　attacker

故意利用技术性和非技术性安全控制措施的脆弱性，以窃取或损害信息系统和网络，或者损害信息系统和网络资源对合法用户的可用性的任何人。

2.2

攻击　attack

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

[GB/T 29246—2017，定义2.3]

2.3

入侵　intrusion

对网络或联网系统的未授权访问，即对信息系统进行有意或无意的未授权访问，包括针对信息系统的恶意活动或对信息系统内资源的未授权使用。

2.4

网络安全事件　cyber security incident

由于自然或者人为以及软硬件本身缺陷或故障的原因，对网络或信息系统造成危害，或对社会造成负面影响的事件。

[GB/T 32924—2016，定义3.4]

注：参考GB/T 20986—2007，网络安全事件包括有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

3　技术类

3.1

有害程序　malware

恶意程序

被专门设计用来损害或破坏系统，对保密性、完整性或可用性进行攻击的程序。

注：有害程序包括病毒、木马、后门、蠕虫等。

3.2

病毒　virus

在计算机程序中插入破坏计算机功能或者数据，影响计算机使用并能自我复制的一组计算机指令