ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1717.2—2020

信息安全技术　网络安全事件通报预警 第2部分：通报预警流程规范

Information security technology—Notification and warning of cyber security incidents—Part 2：Specifications for procedure for notification and warning

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体系技术规范。

本部分为GA/T 1717的第2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。

本部分由公安信息系统安全标准化技术委员会提出并归口。

本部分起草单位：公安部网络安全保卫局、福建省龙岩市公安局网安支队、中科软科技股份有限公司。

本部分主要起草人：黄小苏、张秀东、吴辰苗、任彬、阮晓丽、刘燕岭、赵阳、牟坤。

信息安全技术　网络安全事件通报预警
第2部分:通报预警流程规范

1　范围

GA/T 1717的本部分规定了网络安全事件通报预警的分级和处理流程。

本部分适用于公安机关等相关职能机构或组织开展网络安全事件通报预警工作。

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。凡是注明日期的引用文件,仅注日期的版本适用于本文件,凡是不注明日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/Z 20986—2007　信息安全技术　信息安全事件分类分级指南

GB/T 22240　信息安全技术　信息系统安全等级保护定级指南

GB/T 25069—2010　信息安全技术　术语

GB/T 32924—2016　信息安全技术　网络安全预警指南

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

3　术语和定义

GA/T 1717.1—2020界定的术语和定义适用于本文件。

4　网络安全事件分级

4.1　分级要素

4.1.1　概述

网络安全事件的分级主要考虑两个要素:网络安全保护对象的重要程度和可能受到损害的程度。

4.1.2　网络安全保护对象的重要程度

网络安全保护对象的重要程度根据其所承载的业务对国家安全、经济建设、社会活动的重要性、网络安全等级保护的级别、数据的重要性及敏感程度等综合因素,划分为特别重要、重要和一般三个级别。具体为:

a)　特别重要的保护对象,包括:

1)　重大活动期间的网络安全保护对象;

2)　按照GB/T 22240的规定定级为四级及四级以上的信息系统;

3)　用户量亿级或日活跃用户千万级的互联网重要应用;

4)　日交易量亿元级的电子交易平台;

5)　行业占有率前五的互联网重要应用;

6)　涉及百万级以上公民个人信息的系统;