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;

7） 提供互联网支撑服务的重要系统，如域名解析服务；
8） 由多个重要的网络安全保护对象共同组成的群体；
9） 其他与国家安全关系密切，或与经济建设、社会活动关系非常密切的系统。

b） 重要的保护对象，包括：
1） 按照 GB/T 22240 的规定定级为三级的信息系统；
2） 用户量千万级或日活跃用户百万级的互联网重要应用；
3） 行业占有率较高的互联网应用；
4） 涉及十万级以上，百万级以下公民个人信息的系统；
5） 由多个一般的网络安全保护对象共同组成的群体；
6） 与国家安全密切程度较小，或与经济建设、社会活动关系密切的系统。

c） 一般的保护对象，包括：
1） 按照 GB/T 22240 的规定定级为二级及二级以下的信息系统；
2） 其他公共互联网服务等。

4.1.3 网络安全保护对象可能受到损害的程度

网络安全保护对象受到损害的程度是指网络安全事件或威胁对其软硬件、功能及数据的损坏，导致业务系统运行缓慢或中断，数据泄露、篡改、丢失或损坏，对保护对象造成直接或间接损失的程度。划分为特别严重、严重、较大和一般四个级别。具体为：

a） 特别严重的损害，是指可能造成或已造成网络或信息系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除负面影响所需付出的代价十分巨大。包括但不限于：
1） 大规模、持续性的网络攻击，可能造成或已造成网络或信息系统大面积瘫痪，使其丧失业务处理能力；
2） 波及一个或多个省市的大部分地区，极大威胁国家安全，引起社会动荡，对经济建设有极其恶劣的负面影响，或者严重损害公众利益；
3） 遭受网络攻击后，可能造成或已经造成大量重要信息泄露。

b） 严重的损害，是指可能造成或已造成网络或信息系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大。包括但不限于：
1） 较大规模、持续时间较短的攻击，可能造成或已造成网络或信息系统中断或局部瘫痪，使其业务处理能力受到极大影响；
2） 波及一个或多个地市的大部分地区，威胁到国家安全，引起社会恐慌，对经济建设有重大的负面影响，或者损害到公众利益；
3） 遭受网络攻击后，可能造成或已造成重要信息泄露。

c） 较大的损害，是指可能造成或已造成网络或信息系统中断，明显影响系统效率，使其业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除负面影响所需付出的代价较大。包括但不限于：
1） 较小规模、非持续性的攻击，可能造成或已造成保护对象网络或系统中断，明显影响系统效率，使其业务处理能力受到极大影响；
2） 波及一个或多个地市的部分地区，可能影响到国家安全，扰乱社会秩序，对经济建设有一定的负面影响，或者影响到公众利益；
3） 遭受网络攻击后，可能造成或已造成敏感信息泄露。

d） 一般的损害，是指可能造成或已造成网络或信息系统短暂中断，影响系统效率，使系统业务处

理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除负面影响所需付出的代价较小。包括但不限于：

1） 无规模、非持续性的攻击，造成保护对象网络和系统短暂中断，影响系统效率，使其业务处理能力受到影响；

2） 波及到一个地市的部分地区，对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益会造成损害；

3） 遭受网络攻击后，可能造成或已造成个人信息泄露。

4.2 网络安全事件通报分级

4.2.1 概述

根据网络安全事件的分级要素，将网络安全事件通报划分为四个级别：Ⅰ级事件通报、Ⅱ级事件通报、Ⅲ级事件通报和Ⅳ级事件通报。

4.2.2 Ⅰ级事件通报

能够导致特别严重影响或破坏的网络安全事件，包括以下情况：

a） 涉及国家政治安全的网络安全事件；

b） 涉及恐怖活动的网络安全事件；

c） 对特别重要网络安全保护对象产生特别严重或严重的损害。

4.2.3 Ⅱ级事件通报

能够导致严重影响或破坏的网络安全事件，包括以下情况：

a） 对特别重要网络安全保护对象产生较大或一般的损害；

b） 对重要网络安全保护对象产生特别严重或严重的损害。

4.2.4 Ⅲ级事件通报

能够导致较大影响或破坏的网络安全事件，包括以下情况：

a） 对重要网络安全保护对象产生较大或一般的损害；

b） 对一般网络安全保护对象产生特别严重或严重的损害。

4.2.5 Ⅳ级事件通报

能够导致一般影响或破坏的网络安全事件，对一般网络安全保护对象产生较大或一般的损害。

4.2.6 网络安全事件通报级别表

由网络安全保护对象的重要程度和网络安全保护对象可能或已受到损害的程度确定的网络安全事件通报级别见表1。

表1 网络安全事件通报级别

网络安全保护对象的重要程度	网络安全保护对象可能受到损害的程度			
	特别严重	严重	较大	一般
特别重要	Ⅰ级事件通报	Ⅰ级事件通报	Ⅱ级事件通报	Ⅱ级事件通报
重要	Ⅱ级事件通报	Ⅱ级事件通报	Ⅲ级事件通报	Ⅲ级事件通报

表 1（续）

网络安全保护对象的重要程度	网络安全保护对象可能受到损害的程度			
	特别严重	严重	较大	一般
一般	Ⅲ级事件通报	Ⅲ级事件通报	Ⅳ级事件通报	Ⅳ级事件通报

4.3 网络安全事件预警分级

根据 GB/T 32924—2016 中 4.2 的规定，网络安全预警级别分为四个级别：红色预警（Ⅰ级预警）、橙色预警（Ⅱ级预警）、黄色预警（Ⅰ Ⅲ级预警）、蓝色预警（Ⅳ级预警）。

5 通报流程

5.1 通报的发布

5.1.1 网络安全事件通报级别的判定

应根据网络安全保护对象的重要程度和可能受到损害的程度，判定网络安全事件通报的级别。

5.1.2 通报发布

通报发布应包括但不限于以下内容：

a） 根据网络安全事件通报的级别及时向被通报单位发布网络安全事件通报；

b） 汇总分析近期发生的网络安全事件，并发布网络安全事件分析报告。包括：周报、月报、年报、期刊等。

5.1.3 通报方式

通报发布的方式主要包括：通报平台、传统文件、互联网及其他即时通信工具等。

5.1.4 通报内容

网络安全事件通报的内容应包括但不限于以下：事件级别、威胁类型、事件截图、发现时间、涉及对象、威胁方式、严重程度、防范措施及建议等信息。通报内容见附录 A 中的 A.1。

5.2 通报的处置

5.2.1 通报的处置时限

通报的处置时限见表 2。

表 2 通报处置时限

级别	处置时限
Ⅰ级事件通报	a） 被通报单位接到Ⅰ级事件通报，应立即启动网络安全事件处置工作； b） 应在 5 个工作日内完成安全事件处置工作，并将网络安全事件总结报告上报上级主管单位
Ⅱ级事件通报	a） 被通报单位接到Ⅱ级事件通报，应在 12 h 内启动网络安全事件处置工作； b） 应在 10 个工作日内完成安全事件处置工作，并将网络安全事件总结报告上报通报单位

表 2（续）

级别	处置时限
Ⅲ级事件通报	a） 被通报单位接到Ⅲ级或Ⅳ级事件通报，在 24 h 内启动网络安全事件处置工作； b） 应在 15 个工作日内完成安全事件处置工作，并将网络安全事件总结报告上报通报单位
Ⅳ级事件通报	

5.2.2 通报的处置

通报的处置由调查与分析和网络安全事件处置两个部分组成：

a） 调查与分析：

1） 针对网络安全事件通报内容，对系统内存在的安全威胁进行调查和分析，确认网络安全事件对业务的影响范围和程度，分析对网络安全事件进行响应恢复所需要的时间；

2） 根据网络安全事件造成的损失程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素，确定网络安全事件级别，制定网络安全事件报告程序；

3） 上报内容应包括但不限于：事件的级别、类型、产生原因、敏感程度、影响范围及与事件通报相关的基本信息（单位信息、软硬件信息、人员信息等）。分析报告内容见附录 A 中 A.2。

b） 网络安全事件处置：

1） 根据网络安全事件的级别，制定网络安全事件处置方案，包括网络安全事件处置方法以及应采取的防范措施，并按照网络安全事件处置流程和方案对网络安全事件进行处置；

2） 在事件处置过程中，应根据网络安全事件的级别和严重程度，开展网络安全事件现场线索初查、安全评估及现场保护工作，及时提取固定电子证据。

5.2.3 通报的总结和报告

通报的总结和报告应包括但不限于以下内容：

a） 网络安全事件处置完成后，分析网络安全事件处置记录，并对网络安全事件处置过程进行总结，制定网络安全事件处置报告，向上级主管部门和网络安全通报发布机构上报；

b） 网络安全事件处置报告应包括但不限于：被通报单位基本信息、被通报系统基本信息、分析结果和处置结果。总结报告内容见附录 A 中 A.3。

5.3 通报的归档

应按事件级别和类型分类进行归档，归档事件应包括以下内容：

a） 事件级别；

b） 事件类型；

c） 关键阶段成果描述；

d） 关键阶段完成时间；

e） 处置结果。

6 预警流程

6.1 预警的发布

网络安全预警由国家授权的预警发布机构发布。网络安全预警发布内容包括事件级别、威胁方式、

影响范围、涉及对象、严重程度、防范措施及建议等信息。

6.2 预警的处置

网络与信息系统的主管和运营部门接到网络安全预警后，应进行如下操作：

a） 分析、研判相关事件或威胁对自身网络安全保护对象可能造成损害的程度；

b） 将研判结果向上级及主管部门汇报；

c） 经上级及主管部门同意后，采取适当形式发送预警或通告相关用户；

d） 根据情况启动应急预案。

当可能对网络与信息系统保护对象产生特别严重的损害时，网络与信息系统的主管或运营部门应及时向单位负责人和网络安全第一责任人汇报。

6.3 预警的升级或降级

预警发布机构根据网络安全事件或威胁的动态变化，及时发布预警的升级或降级信息。

6.4 预警的解除

当网络安全威胁情况消除或威胁达不到蓝色预警（Ⅳ级预警）级别，预警发布机构应及时解除预警。

7 评价指标

为提高网络安全事件处置的质量和效率，可建立相应评价指标体系，评价指标宜涵盖处置事件数量、处置完成率、处置质量等信息。

附 录 A
（规范性附录）
网络安全事件通报内容、报告及分级示例说明

A.1 网络安全事件通报内容

网络安全事件通报内容见表 A.1。

表 A.1 网络安全事件通报内容

序号	项目	说明	备注
1	事件编号	唯一的标识，依据规则创建	必选项
2	事件级别	（Ⅰ、Ⅱ、Ⅲ、Ⅳ）/级	必选项
3	事件类型	指通报事件的类型，依据 GB/Z 20986 事件类型分为：隐患类事件、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、其他事件。 应对事件类型进一步细化，如，隐患类事件可分为：SQL 注入漏洞、弱口令漏洞、跨站脚本漏洞等。网络攻击事件可分为：拒绝服务攻击事件、后门攻击事件等	必选项
4	网站/系统名称	网站/系统的中文标识	如果事件涉及网站/系统，此项为必选项，其他情况下为非必选项
5	威胁 URL	存在威胁或遭受入侵的目标 URL 地址	如果事件涉及具体 URL，此项为必选项，其他情况下为非必选项
6	IP 地址	存在威胁或遭受入侵的物理 IP 地址	非必选项
7	发现时间	YYYY-MM-DD hh：mm：ss	必选项
8	备案信息	公安备案或工信部备案信息	如果为备案网站/系统此项为必选项、其他情况下为非必选项
9	管辖地域	被通报单位所在的备案或行政辖区	必选项
10	所属行业	被通报单位的行业类别	必选项
11	隶属单位	网站/系统的主办单位	必选项
12	事件描述	详细描述事件的发现过程及现有状态，可使用文字＋截图的形描述	必选项
13	严重程度	事件可能造成的或已经造成的损害程度	非必选项
14	防范措施及建议	针对事件给出的解决方法及相关处置建议	非必选项

表 A.1（续）

序号	项目	说明	备注
15	其他	其他内容	非必选项
注：可根据实际业务需求做适当变更。			

A.2 网络安全事件分析报告

网络安全事件分析报告内容见表 A.2。

表 A.2 网络安全事件分析报告

序号	项目	说明	备注
1	事件级别	（Ⅰ、Ⅱ、Ⅲ、Ⅳ）/级	
2	备案信息	公安备案或工信部备案信息	
3	事件类型	事件的类型	
4	产生原因	事件产生的具体因素	
5	敏感程度		
6	影响范围		
7	单位信息		
8	系统硬件信息		
9	系统软件信息		
10	运维人员信息		
11	其他		

A.3 网络安全事件总结报告

网络安全事件总结报告内容见表 A.3。

表 A.3 网络安全事件总结报告

序号	项目	说明	备注
1	被通报单位基本信息	单位名称、单位地址、单位性质、所属行业、单位法人等	
2	被通报系统基本信息	系统名称、系统域名、等级保护备案信息、硬件部署信息、系统开发单位、安全服务商、系统负责人等信息	

表 A.3（续）

序号	项目	说明	备注
3	分析结果	事件的级别、类型、产生原因、敏感程度、影响范围、后续响应方案等信息	
4	处置结果	处置方法、防范措施、关键过程节点记录等信息	
5	威胁样本		
6	事件日志		
7	处置文件复印件	处置过程文件复印件	

A.4 网络安全事件通报分级示例

某连锁酒店企业存在安全漏洞，造成5亿条公民个人信息泄露事件，涉及旗下多个酒店品牌，全国范围受到影响。

此次网络安全事件通报分级情况如下：

a） 此单位属于国内酒店集团规模排行第三的企业，且用户量超过亿级，根据4.1.2规定，应划分为“特别重要的保护对象”；

b） 此次事件造成5亿条个人信息泄露，涉及全国范围，根据4.1.2规定，应划分为“特别严重的损害”。

根据以上分析结果，通过“网络安全事件通报级别表”判定此次网络安全事件的通报级别为“Ⅰ级事件通报”。

参 考 文 献

[1] GB/Z 20986—2007 信息安全技术 信息安全事件分类分级指南
[2] GB/T 25069—2010 信息安全技术 术语

中华人民共和国公共安全
行业标准
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
GA/T 1717.2—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址：www.spc.org.cn
服务热线：400-168-0010
2020年10月第一版
*
书号：155066·2-35546

GA/T 1717.2-2020