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

或者程序代码。

[GB/T 31499—2015,定义 3.6]

3.3

蠕虫 worm

通过信息系统或计算机网络进行自身传播,从而造成恶意占用可用资源等损害的有害程序。

注:改写 GB/T25069—2010,定义 2.1.26。

3.4

特洛伊木马 trojan horse

伪装成良性应用程序的有害程序。

注:简称木马。

3.5

后门 backdoor

绕过了系统的安全策略,可以对程序、系统进行访问、控制的程序或代码。

3.6

网页后门 webshell

以网页文件形式存在的命令执行环境。

3.7

间谍软件 spyware

从计算机用户收集私人或保密信息的欺骗性软件。

3.8

勒索软件 ransomware

以勒索财物等为目的,通过技术手段阻碍用户正常使用计算机软件、数据等资源的有害程序。

3.9

破坏性程序 destructive program

具有对计算机信息系统的功能或存储、处理及传输的数据进行非授权获取、删除、增加、修改、干扰、破坏等功能的有害程序。

3.10

恶意 IP 地址 malicious IP

蓄意传播病毒、木马等有害程序,或在网络攻击活动中使用的 IP 地址。

3.11

恶意域名 malicious domain name

蓄意传播有害内容、有害程序,或在网络攻击活动中使用的域名。

3.12

隐患 potential hazard

在网络空间环境下的技术、管理等方面存在的潜在危害。

3.13

漏洞 vulnerability

计算机信息系统在需求、设计、实现、配置、运行等过程中,有意或无意产生的缺陷。这些缺陷以不同形式存在于计算机信息系统的各个层次和环节之中,一旦被恶意主体所利用,就会对计算机信息系统的安全造成损害,从而影响计算机信息系统的正常运行。

[GB/T 28458—2012,定义 3.2]

3.14

漏洞等级 vulnerability level

根据漏洞的影响对象、影响范围、利用难度、造成的后果等要素划分的危害级别。一般分为高危、中

危和低危漏洞。

3.15

通用型漏洞　universal vulnerability

通用软硬件的漏洞。

3.16

事件型漏洞　incident vulnerability

不具有通用性，对特定信息系统或网络构成安全威胁的漏洞。

3.17

扫描　scan

对网络上的网络设备、主机和应用进行鉴识的过程，是进行网络安全评估或实施网络攻击的前提之一。

注：改写 GB/T 25069—2010，定义 2.2.1.109。

3.18

嗅探　sniff

通过程序或设备捕获网络中的信息。

注：改写 GB/T 25069—2010，定义 2.2.1.120。

3.19

渗透　penetration

绕过信息系统安全机制的未授权行为。

3.20

暴力破解　brute force

针对密码或身份认证等进行穷举尝试，试图破解加密信息，突破认证方式的方法。

3.21

僵尸网络　botnet

被攻击者集中控制的大量主机或网络设备，可被用于发动大规模恶意活动，如分布式拒绝服务攻击等。

3.22

攻击模式　attack pattern

针对应用程序或系统的攻击方法的抽象。

注：例如 SQL 注入攻击、中间人攻击、会话劫持等。

3.23

漏洞利用　vulnerability exploit

通过漏洞试图获取系统权限、数据资源的技术或代码，通常采用脚本形式。

3.24

注入　injection

将一些包含指令的数据发送到解释程序中，使得解释程序将收到的数据转换为指令执行，导致数据破坏、泄露，权限绕过等。

3.25

SQL 注入　SQL injection；structured query language(SQL) injection

通过将一些恶意的 SQL 命令作为参数传递到应用程序中，欺骗数据库执行恶意命令的攻击方式，可导致数据窃取、更改、删除等后果。

3.26

跨站脚本攻击　cross-site scripting attack

攻击者通过向目标网站注入恶意代码，从而对此网站的用户发起攻击的攻击行为。可造成 Cookie

资料窃取、会话劫持、钓鱼欺骗等后果。

3.27

命令执行攻击　command execution attack

命令注入

利用应用程序中对用户提交数据验证不足的缺陷，通过构造特殊命令字符串，提交到系统 shell 中执行。

3.28

代码执行攻击　code execution attack

代码注入

利用应用程序缺乏输入、输出数据验证的缺陷，通过构造恶意代码，提交应用程序中执行。

3.29

URL 跳转攻击　URL jump attack；Uniform Resource Locator（URL）jump attack

URL 重定向攻击

利用应用程序未对传入的 URL 变量进行检查的缺陷，构造恶意 URL，诱导用户跳转到恶意网站。

3.30

缓冲区溢出攻击　buffer overflow attack

向缓冲区内填充数据超过缓冲区本身的容量，导致数据溢出到被分配空间之外的内存空间，使得溢出的数据覆盖了其他内存空间数据的攻击方式。

3.31

目录遍历攻击　directory traversal attack

利用服务端安全认证缺失等缺陷，使得服务端文件操作接口执行了遍历目录的恶意代码，访问受限制的目录。

3.32

文件包含攻击　file include attack

利用系统对用户可控参数过滤不严的缺陷，将构造的代码传递给包含函数的行为。

注：可导致信息泄露、执行任意代码等。

3.33

文件上传攻击　file upload attack

利用应用程序对上传文件过滤不严的缺陷，上传应用程序定义类型范围之外的文件到服务端。

注：例如上传一个网页后门（webshell）到具有执行脚本权限的目录中。

3.34

文件下载攻击　file download attack

利用应用程序对可下载的文件缺乏限制的缺陷，查看或下载任意文件。

注：例如系统配置文件、敏感文件等。

3.35

拒绝服务　Denial of Service；DoS

阻止对系统资源的授权访问或延迟系统的运行和功能，并导致授权用户可用性降低的行为。

3.36

分布式拒绝服务攻击　DDoS attack；Distributed Denial of Service（DDoS）attack

将大量主机或网络设备联合起来作为攻击平台，对一个或多个目标发起的拒绝服务攻击。

3.37

泛洪攻击　flooding attack

洪水攻击

向目标主机发送大量无用数据报文，造成目标主机无法提供正常服务的网络攻击。

3.38

跨站请求伪造　cross-site request forgery

利用浏览器能保存会话 cookie 等凭证，并会自动发送的特点，攻击者以受害者名义伪造请求并发送给受攻击的网页，能以受害者的身份和权限执行一些特殊敏感的操作。

3.39

劫持　hijack

通过拦截或篡改信息，造成用户不能访问目标或访问虚假、伪造信息的攻击方式。

注：例如会话劫持、浏览器劫持、域名劫持、流量劫持等。

3.40

域名劫持　DNS hijack；Domain Name System（DNS）hijack

通过篡改域名解析记录或拦截域名解析请求等方式，造成用户访问虚假网站或不能访问特定网站的行为。

3.41

网页篡改　Web tamper

对网站展示的页面内容进行非授权的增加、修改、删除、变造等的行为。

3.42

网络钓鱼　phishing

通过在电子通信中伪装成可信赖的实体来尝试获取隐私或保密信息的欺诈性过程。

3.43

社会工程学攻击　social engineering attack

以心理学等社会科学为主要手段收集信息、情报的方法。

注：例如目标刻画、钓鱼欺骗、伪装假冒等。

3.44

网络资产　cyber asset

计算机系统和网络中使用的软硬件、数据和服务。

3.45

设备指纹　device fingerprint

在网络中能够唯一识别出设备的独特的数字特征或标识。

3.46

网络流量　network traffic

在网络中传输的数据包的集合。

3.47

日志　log

计算机设备或软件系统的运行记录。

注：包括系统日志、网络日志等。

3.48

系统日志　system log

由操作系统、应用程序自身生成，记录系统运行情况的日志。

3.49

网络日志　network log

由网络流量中提取的元数据信息生成，记录网络状态、活动、行为等的日志。

注：元数据信息是指五元组、七元组等信息。

3.50

审计日志　audit log

为了发现违规、异常等情况，记录特定行为的日志。

注：例如登录、注销、修改、删除等行为。

3.51

通联日志　communication log

记录网络会话而生成的日志。

注：通常包括时间、源 IP 地址、源端口、目的 IP 地址、目的端口和传输层协议等。

3.52

管理端口远程连接日志　management port remote connection log

通过网络对管理端口进行访问而生成的日志。

注：主要指远程桌面、SSH、Telnet 和 FTP 等产生的日志。

4　业务类

4.1

网络安全保护目标　target of cyber security protection

涉及国家安全、社会秩序、公共利益及公民、法人和其他组织的合法权益的计算机系统、网络和数据。

4.2

重要信息系统　critical information system

关系国家安全、经济命脉、社会稳定的信息系统。

[GB/T 31495.2—2015，定义 3.2]

4.3

重要数据　critical data

重要信息系统中存储、交换、传输、处理的数据，以及与国家安全、社会秩序、公共利益密切相关的数据。

4.4

有害程序事件　malware incident

蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的网络安全事件。

4.5

网络攻击事件　cyber attack incident

利用信息系统或网络的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统或网络实施攻击，并造成系统异常或对系统当前运行造成潜在危害的网络安全事件。

4.6

信息破坏事件　information destroy incident

通过网络或其他技术手段，造成信息系统或网络中的信息被篡改、假冒、泄漏、窃取等而导致的网络安全事件。

4.7

信息内容安全事件　information content security incident

利用信息网络发布、传播危害国家安全、社会稳定和公共利益内容的网络安全事件。

4.8

设备设施故障事件　cyber facility fault incident

由于信息系统和网络自身故障或外围保障设施故障而导致的网络安全事件，以及人为的使用非技

术手段有意或无意的造成系统破坏而导致的网络安全事件。

4.9

灾害性事件　disaster incident

由于不可抗力对信息系统或网络造成物理破坏而导致的网络安全事件。

4.10

威胁　threat

可能对系统或组织造成经济损失、负面影响等损害的风险来源。

注：改写 GB/T 29246—2017，定义 2.83。

4.11

威胁信息　threat information

与威胁相关的，人、地、物、事、组织等信息，可描述现有或可能出现的威胁，从而实现对威胁的响应和预防。

注：改写 GB/T36643—2018，定义 3.3。

4.12

预警　warning

针对即将发生或正在发生的网络安全事件或威胁，提前或及时发出的安全警示。

[GB/T 32924—2016，定义 3.5]

4.13

通报　notification

为及时发现网络安全保护目标的风险和隐患，妥善处置网络安全事件而开展的重要工作。

注：通报是国家网络与信息安全信息通报工作的重要组成部分。

4.14

处置　disposal

根据网络安全事件的类型和级别，由公安机关等执法部门依法开展的监督管理、执法检查和侦查调查等工作。

4.15

网络安全态势感知　cyberspace situation awareness

在大规模网络环境中，对引起网络安全态势发生变化的所有要素按照一定规则进行感知和收集，获得网络的整体安全状况及应对措施，对网络安全状况的发展趋势进行预测的过程。

注：网络安全态势感知的目的是及时发现重大网络安全事件，精准防护关键信息基础设施，精确打击网络违法犯罪活动。

4.16

追踪溯源　traceability

根据证据重现网络攻击事件，包括攻击组织、方式、路径、资源等，并挖掘网络攻击活动有关的人、地、事、物、组织等的过程。

4.17

审计踪迹　audit trail

按事件顺序检查、审查、检验其运行环境及相关事件活动的过程。主要用于实现重现事件、评估损失、检测系统产生的问题区域、提供有效的应急灾难恢复、防止系统故障或使用不当等方面。

[GB/T 25069—2010，定义 2.2.1.103]

汉语拼音索引

X

Y

Z

英语对应词索引

H

I

L

M

N

P

R

S

T

U

V

W

参 考 文 献

[1] GB/Z 20985 信息安全技术 信息安全事件管理指南

[2] GB/Z 20986 信息安全技术 信息安全事件分类分级指南

[3] GB/T 28458—2012 信息安全技术 安全漏洞标识与描述规范

[4] GB/T 29246—2017 信息技术 安全技术 信息安全管理体系概述和词汇

[5] GB/T 31495.2—2015 信息安全技术 信息安全保障指标体系及评价方法 第2部分:指标体系

[6] GB/T 31499—2015 信息安全技术 统一威胁管理产品技术要求和测试评价方法

[7] GB/T 32924—2016 信息安全技术 网络安全预警指南

[8] GB/T 36643—2018 信息安全技术 网络安全威胁信息格式规范

[9] ISO/IEC 27039:2016 Information technology—Security techniques—Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

[10] ISO/IEC 27033-1:2015 Information technology—Security techniques —Network security—Part 1:Overview and concepts

[11] ISO/IEC 27032:2012 Information technology—Security techniques—Guidelines for cybersecurity

[12] ITU-T x.1544 Common attack pattern enumeration and classification

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1部分：术语
GA/T 1717.1—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：155066·2-35547

GA/T 1717.1-2020