ICS 35.40
L80

中华人民共和国国家标准

GB/T 22240—20XX
代替 GB/T 22240-2008

信息安全技术
网络安全等级保护定级指南

Information security technology-
Guidelines for grading of classified cybersecurity protection

（试行稿）

（本稿完成日期：2017.10.25）

20XX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T1.1—2009给出的规则起草。

本标准代替GB/T 22240—2008《信息安全技术　信息系统安全等级保护定级指南》，与GB/T 22240—2008相比，主要技术变化如下：

——标准名称变更为《信息安全技术 网络安全等级保护定级指南》。

——修改了等级保护对象、增加了网络、基础信息网络等术语定义（见3,2008版的3）。

——修改了定级要素与安全保护等级的关系（见4.3,2008版4.3）。

——增加了基础信息网络的定级对象确定方法（见5.1）。

——增加了特定定级对象定级说明（见6.5）。

——修改了定级流程（见4.4,2008版5.1）。

本标准由全国信息安全标准化技术委员会提出。

本标准由全国信息安全标准化技术委员会归口。

本标准起草单位：亚信科技（成都）有限公司、公安部信息安全等级保护评估中心和阿里云计算有限公司、深圳市腾讯计算机系统有限公司、启明星辰信息技术集团有限公司等。

本标准主要起草人：李明、曲洁、张振峰、任卫红、袁静、朱建平、马力、刘东红、王欢、沈锡镛杨晓光、段伟恒。

引　言

为了贯彻落实《中华人民共和国网络安全法》，特别是配合网络安全等级保护制度的落地实施，需对GB/T 22240—2008进行修订。从标准名称、等级保护对象定义、安全保护等级描述以及定级流程等方面进行补充、细化和完善，从而满足移动互联、云计算、大数据、物联网和工业控制等新技术、新应用情况下开展网络安全等级保护工作的需要。

与本标准相关的国家标准包括：

——GB/T 22239 信息安全技术 网络安全等级保护基本要求；

——GB/T 25058 信息安全技术 网络安全等级保护实施指南；

——GB/T 28448 信息安全技术 网络安全等级保护测评要求；

——GB/T 28449 信息安全技术 网络安全等级保护测评过程指南。

网络安全等级保护定级指南

1 范围

本标准规定了网络安全等级保护的定级方法和定级流程。

本标准适用于指导网络运营者开展等级保护对象的定级工作。

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 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 25069-2010 信息安全技术 术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 31167 信息安全技术 云计算服务安全指南

3 术语和定义

GB17859-1999、GB/T 25069-2010、GB/T 22239和GB/T 31167界定的以及下列术语和定义适用于本文件。

3.1

等级保护对象target of classified protection

网络安全等级保护工作的作用对象，主要包括基础信息网络、工业控制系统、云计算平台、物联网、使用移动互联技术的网络、其他网络以及大数据等。

3.2

基础信息网络 basic information network

为信息流通、网络运行等起基础支撑作用的网络设备设施，包括电信网、广播电视传输网、互联网、业务专网等。

3.3

网络 network

由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

3.4

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、金融、交通、水利、公共服务和电子政务等重要行业和领域以及其他一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生和公共利益的网络。

3.5

大数据平台 big data platform

采用分布式存储和计算技术，提供大数据的访问、处理和存储，支撑大数据应用安全高效运行的软硬件集合。

3.6

客体object

受法律保护的、等级保护对象受到破坏时所侵害的社会关系。

3.7

客观方面 objective

对客体造成侵害的客观外在表现，包括侵害方式和侵害结果等。

4 定级原理及流程

4.1 安全保护等级

根据等级保护相关管理文件，等级保护对象的安全保护等级分为以下五级：

a) 第一级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益；
b) 第二级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全；
c) 第三级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，或者对社会秩序和公共利益造成严重损害，或者对国家安全造成损害；
d) 第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害；
e) 第五级，等级保护对象受到破坏后，会对国家安全造成特别严重损害。

4.2 定级要素

4.2.1 定级要素概述

等级保护对象的级别由两个定级要素决定：

a) 受侵害的客体；
b) 对客体的侵害程度。

4.2.2 受侵害的客体

等级保护对象受到破坏时所侵害的客体包括以下三个方面：

a) 公民、法人和其他组织的合法权益；

b） 社会秩序、公共利益；

c） 国家安全。

侵害国家安全的事项包括以下方面：

——影响国家政权稳固和主权完整；

——影响国家统一、民族团结和社会稳定；

——影响国家经济秩序和文化实力；

——影响宗教活动秩序和反恐能力建设；

——其他影响国家安全的事项。

侵害社会秩序的事项包括以下方面：

——影响国家机关社会管理和公共服务的工作秩序；

——影响各种类型的经济活动秩序；

——影响各行业的科研、生产秩序；

——影响公众在法律约束和道德规范下的正常生活秩序等；

——其他影响社会秩序的事项。

侵害公共利益的事项包括以下方面：

——影响社会成员使用公共设施；

——影响社会成员获取公开信息资源；

——影响社会成员接受公共服务等方面；

——其他影响公共利益的事项。

侵害公民、法人和其他组织的合法权益是指由法律确认的并受法律保护的公民、法人和其他组织所享有的一定的社会权利和利益等受到损害。

4.2.3 对客体的侵害程度

对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此，对客体的侵害外在表现为对等级保护对象的破坏，通过危害方式、危害后果和危害程度加以描述。

等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：

a） 造成一般损害；

b） 造成严重损害；

c） 造成特别严重损害。

三种侵害程度的描述如下：

——一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害；

——严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害；

——特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常严重损害。

4.3 定级要素与安全保护等级的关系

定级要素与安全保护等级的关系如表1所示。

表1 定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

4.4 定级流程

等级保护对象定级工作的一般流程如图1所示：

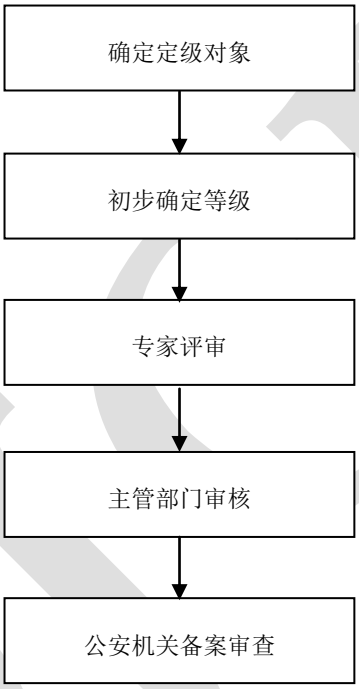


图1 等级保护对象定级工作一般流程

各级等级保护对象定级工作具体要求参见附录B。

5 确定定级对象

5.1 定级对象的基本特征

作为定级对象的网络应具有如下基本特征：

a) 具有确定的主要安全责任主体；

b) 承载相对独立的业务应用；

c) 包含相互关联的多个资源。

注1：主要安全责任主体包括但不限于企业、机关和事业单位等法人，以及不具备法人资格的社会团体等其他组织；

注2：应避免将某个单一的系统组件，如服务器、终端或网络设备作为定级对象。

在确定定级对象时，基础信息网络、工业控制系统、云计算平台、物联网、采用移动互联技术的网络和大数据在满足以上基本特征的基础上，还应分别遵循5.2、5.3、5.4、5.5、5.6和5.7的相关要求。

5.2 基础信息网络

对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。

跨省业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。

5.3 工业控制系统

工业控制系统主要包括现场采集/执行、现场控制、过程控制和生产管理等特征要素。其中，现场采集/执行、现场控制和过程控制等要素应作为一个整体对象定级，各要素不单独定级；生产管理要素可单独定级。

对于大型工业控制系统，可以根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。

5.4 云计算平台

在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。

对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。

5.5 物联网

物联网主要包括感知、网络传输和处理应用等特征要素，应将以上要素作为一个整体对象定级，各要素不单独定级。

5.6 采用移动互联技术的网络

采用移动互联技术的网络主要包括移动终端、移动应用、无线网络等特征要素，应与相关有线网络业务系统作为一个整体对象定级。

5.7 大数据

大数据应作为单独定级对象进行定级；安全责任主体相同的大数据、大数据平台和应用可作为一个整体对象定级。

6 初步确定等级

6.1 定级方法概述

对于一般的网络，其定级方法应按照以下描述进行；对于基础信息网络、云计算平台和大数据平台等起支撑作用的网络，其定级方法应参照6.5。

定级对象的安全主要包括业务信息安全和系统服务安全,与之相关的受侵害客体和对客体的侵害程度可能不同，因此，安全保护等级也应由业务信息安全和系统服务安全两方面确定。从业务信息安全角度反映的定级对象安全保护等级称业务信息安全保护等级；从系统服务安全角度反映的定级对象安全保护等级称系统服务安全保护等级。

定级方法如下：

a) 确定受到破坏时所侵害的客体

1) 确定业务信息受到破坏时所侵害的客体；

2) 确定系统服务受到侵害时所侵害的客体。

b） 确定对客体的侵害程度

1） 根据不同的受侵害客体，分别评定业务信息安全被破坏对客体的侵害程度；

2） 根据不同的受侵害客体，分别评定系统服务安全被破坏对客体的侵害程度。

c） 确定安全保护等级

1） 确定业务信息安全保护等级；

2） 确定系统服务安全保护等级；

3） 将业务信息安全保护等级和系统服务安全保护等级的较高者初步确定为定级对象的安全保护等级。

定级方法的流程示意图参见附录 A。

6.2 确定受侵害的客体

定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。

确定受侵害的客体时，应首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公众利益，最后判断是否侵害公民、法人和其他组织的合法权益。

6.3 确定对客体的侵害程度

6.3.1 侵害的客观方面

在客观方面，对客体的侵害外在表现为对定级对象的破坏，其危害方式表现为对信息安全的破坏和对网络服务的破坏，其中信息安全是指确保网络内信息的保密性、完整性和可用性等，系统服务安全是指确保定级对象可以及时、有效地提供服务，以完成预定的业务目标。由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种危害方式。

业务信息安全和系统服务安全受到破坏后，可能产生以下危害后果：

——影响行使工作职能；

——导致业务能力下降；

——引起法律纠纷；

——导致财产损失；

——造成社会不良影响；

——对其他组织和个人造成损失；

——其他影响。

6.3.2 综合判定侵害程度

侵害程度是客观方面的不同外在表现的综合体现，因此，应首先根据不同的受侵害客体、不同危害后果分别确定其危害程度。对不同危害后果确定其危害程度所采取的方法和所考虑的角度可能不同，例如系统服务安全被破坏导致业务能力下降的程度可以从定级对象服务覆盖的区域范围、用户人数或业务量等不同方面确定，业务信息安全被破坏导致的财物损失可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。

在针对不同的受侵害客体进行侵害程度的判断时，应参照以下不同的判别基准：

——如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准；

——如果受侵害客体是社会秩序、公共利益或国家安全，则应以整个行业或国家的总体利益作为判

断侵害程度的基准。

业务信息安全和系统服务安全被破坏后对客体的侵害程度，由对不同危害结果的危害程度进行综合评定得出。由于各行业定级对象所处理的信息种类和系统服务特点各不相同，业务信息安全和系统服务安全受到破坏后关注的危害结果、危害程度的计算方式均可能不同，各行业可根据本行业信息特点和系统服务特点，制定危害程度的综合评定方法，并给出侵害不同客体造成一般损害、严重损害、特别严重损害的具体定义。

6.4 确定安全保护等级

根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表2业务信息安全保护等级矩阵表，即可得到业务信息安全保护等级。

表2 业务信息安全保护等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表3系统服务安全保护等级矩阵表，即可得到系统服务安全保护等级。

表3 系统服务安全保护等级矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

定级对象的安全保护等级由业务信息安全保护等级和系统服务安全保护等级的较高者决定。

6.5 特定定级对象定级说明

对于基础信息网络、云计算平台、大数据平台等支撑类网络，应根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级。

对于大数据，应综合考虑数据规模、数据价值等因素，根据数据资源（完整性、保密性、可用性）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侵害程度等因素确定其安全保护等级。原则上，大数据安全保护等级不低于第三级。

对于确定为关键信息基础设施的，原则上其安全保护等级不低于第三级。

7 专家评审

定级对象的运营、使用单位应组织信息安全专家和业务专家等，对初步定级结果的合理性进行评审，出具专家评审意见。

8 主管部门审核

定级对象的运营、使用单位应将初步定级结果上报行业主管部门或上级主管部门进行审核。

9 公安机关备案审查

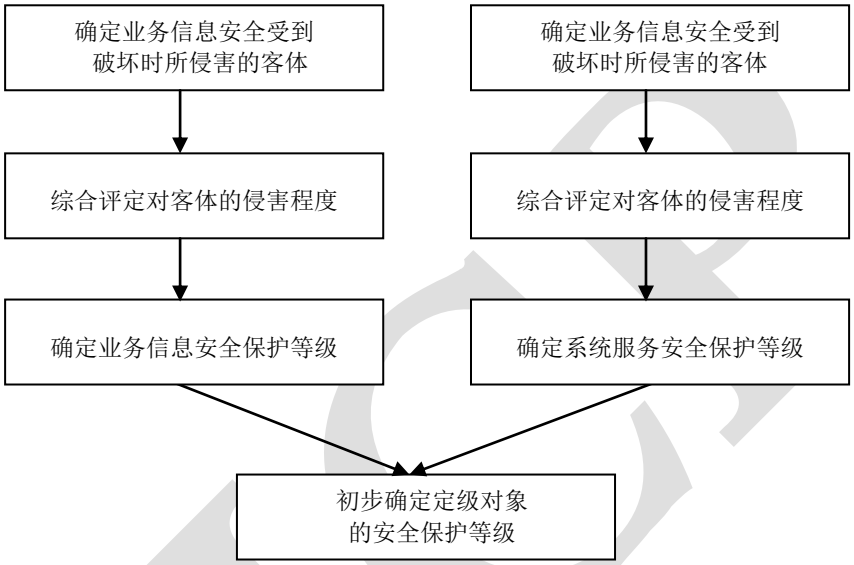
定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，审查不通过，其运营使用单位应组织重新定级；审查通过后最终确定定级对象的安全保护等级。

10 等级变更

当等级保护对象所处理的信息、业务状态和系统服务范围发生变化，可能导致业务信息安全或系统服务安全受到破坏后的受侵害客体和对客体的侵害程度发生变化时，应根据本标准要求重新确定定级对象和安全保护等级。

附 录 A
（资料性附录）
定级方法流程

等级保护对象定级方法流程如图A.1所示：



图A.1 定级方法流程示意图

附 录 B
（资料性附录）
各级等级保护对象定级工作要求

各级等级保护对象定级工作具体要求如下：

a）安全保护等级初步确定为第二级及以上的等级保护对象，其运营使用单位应当依据本标准进行初步定级、专家评审、主管部门审批、公安机关备案审查，最终确定其安全保护等级；

b）安全保护等级初步确定为第四级的等级保护对象，在开展专家评审工作时，其运营使用单位应当请国家信息安全等级保护专家评审委员会进行评审。

参 考 文 献

[1] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

[2] National Institute of Standards and Technology Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.