ICS 35.40
L80

GA

中华人民共和国公共安全行业标准

GA/T 20—XXXX

信息安全技术
网络安全等级保护定级指南

Information security technology-

Classification guide for cyber security classified protection

点击此处添加与国际标准一致性程度的标识

（报批稿）

（本稿完成日期：）

20XX－XX－XX 发布　　20XX－XX－XX 实施

中华人民共和国公安部　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部信息安全等级保护评估中心、电力行业信息安全等级保护测评中心第一测评实验室、阿里云计算有限公司、杭州华三通信技术有限公司。

本标准主要起草人：李明、曲洁、任卫红、张振峰、袁静、朱建平、马力、刘韧、陈雪秀、刘鑫。

引　言

依据《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）和《信息安全等级保护管理办法》（公通字〔2007〕43号）制定本标准。

与本标准相关的国家系列标准包括：

——　GB/T 25058-2010 信息安全技术 信息系统安全等级保护实施指南；

——　GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求；

——　GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评要求。

本标准依据等级保护相关管理文件，综合考虑保护对象在国家安全、经济建设、社会生活中的重要程度，以及保护对象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，提出确定保护对象安全保护等级的方法。

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。

本标准适用于为等级保护对象的定级工作提供指导。

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，仅所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

3 术语和定义

GB17859-1999和GB/T 25069-2010确立的以及下列术语和定义适用于本标准。

3.1

等级保护对象 target of classified protection

网络安全等级保护的保护对象，主要包括基础信息网络、信息系统（诸如传统信息系统、工业控制系统、云计算平台、物联网、使用移动互联技术的信息系统等）和大数据等。

3.2

基础信息网络 foundational information network

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

3.3

信息系统 information system

由计算机和类计算机的软硬件及其相关的和配套的设备、设施构成的，按照一定的应用目标和规则进行信息处理或过程控制的资源集合。

注：资源可以是物理设备，也可以是虚拟设备。

3.4

国家关键信息基础设施 national critical information infrastructure

关系到国家核心利益、人民群众生命财产安全和社会生产生活秩序，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基础信息网络、重要业务系统和生产控制系统以及重要数据资源等。

3.5

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，如国家安全、社会秩序、公共利益以及公民、法人或其他组织的合法权益。

3.6

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：

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。

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。

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。

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。

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国防实力；

——影响国家统一、民族团结和社会安定；

——影响国家对外活动中的政治、经济利益；
——影响国家重要的安全保卫工作；
——影响国家经济竞争力和科技实力；
——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

国家关键信息基础设施的安全保护等级应不低于第三级。

4.4 定级流程

等级保护对象定级的一般流程如下：

a) 确定定级对象；
b) 初步确定等级；
c) 专家评审；
d) 主管部门审核；
e) 公安机关备案审查。

5 确定定级对象

5.1 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。

跨省全国性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。

5.2 信息系统

5.2.1 传统信息系统

作为定级对象的传统信息系统应具有如下基本特征：

a) 具有唯一确定的安全责任单位。作为定级对象的传统信息系统应能够唯一地确定其安全责任单位。如果一个单位的某个下级单位负责信息系统安全建设、运行维护等过程的全部安全责任，则这个下级单位可以成为信息系统的安全责任单位；如果一个单位中的不同下级单位分别承担信息系统不同方面的安全责任，则该信息系统的安全责任单位应是这些下级单位共同所属的单位；
b) 承载相对独立的业务应用。作为定级对象的传统信息系统应承载相对独立的业务应用，完成不同业务目标或者支撑不同单位或不同部门职能的多个信息系统应划分为不同的定级对象；
c) 具有信息系统的基本要素。作为定级对象的传统信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的多资源集合，单一设备（如服务器、终端、网络设备等）不单独定级。

5.2.2 工业控制系统

工业控制系统主要由生产管理层、现场设备层、现场控制层和过程监控层构成，其中：生产管理层的定级对象确定方法参见5.2.1节。现场设备层、现场控制层和过程监控层应作为一个整体对象定级，各层次要素不单独定级。

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

5.2.3 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。

5.2.4 物联网

物联网应作为一个整体对象定级，主要包括感知层、网络传输层和处理应用层等要素。

5.2.5 采用移动互联技术的信息系统

采用移动互联技术的等级保护对象应作为一个整体对象定级，移动终端、移动应用和无线网络等要素不单独定级。

5.3 大数据

应将具有统一安全责任单位的大数据作为一个整体对象定级。

6 初步确定安全保护等级

6.1 定级方法概述

根据定级对象的不同，定级方法主要包括以下三种：

a) 业务处理类定级方法：适用于传统信息系统、工业控制系统、物联网、和采用移动互联技术的信息系统等定级对象；
b) 数据资源类定级方法：适用于大数据等定级对象；
c) 基础支撑类定级方法：适用于基础信息网络和云计算平台等定级对象。

6.2 业务处理类定级方法

6.2.1 方法概述

传统信息系统、物联网、工业控制系统等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，从多个方面综合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，从多个方面综合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) 依据表 2，得到业务信息安全保护等级；
   2) 依据表 3，得到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。

6.2.2 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。

6.2.3 确定对客体的侵害程度

6.2.3.1 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业务信息安全的破坏和对信息系统服务的破坏，其中业务信息安全是指确保信息系统内信息的保密性、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。

6.2.3.2 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。

6.2.4 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。

6.3 数据资源类定级方法

对于大数据等定级对象，应综合考虑数据规模、数据价值等因素根据其在国家安全、经济建设、社会生活中的重要程度，以及数据资源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其安全保护等级，具体方法参见6.2.1节。原则上大数据安全保护等级为第三级以上。

6.4 基础支撑类定级方法

对于基础信息网络、云计算平台等定级对象，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。

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，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

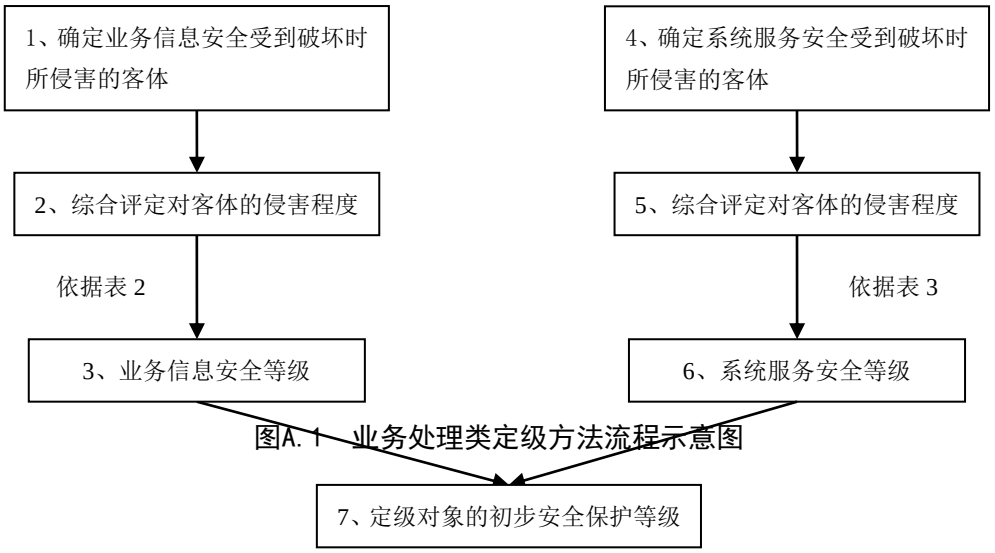
定级对象的运营、使用单位应按照相关管理规定，将初步定级结果提交公安机关进行备案审查，最终确定定级对象的安全保护等级。

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有较大的变化时，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）
业务处理类定级方法流程

业务处理类定级方法流程如下图所示：



图A.1 业务处理类定级方法流程示意图

参 考 文 献

[1] GB/T 22239（所有部分）信息安全技术 网络安全等级保护基本要求
[2] GB/T 31167-2014 信息安全技术 云计算服务安全指南
[3] GB/T 31168-2014 信息安全技术 云计算服务安全能力要求
[4] 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.