ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22240—2008

信息安全技术
信息系统安全等级保护定级指南

Information security technology—
Classification guide for classified protection of information system security

2008-06-19 发布　　2008-11-01 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

本标准由公安部和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：公安部信息安全等级保护评估中心。

本标准主要起草人：任卫红、曲洁、马力、朱建平、李明、李升、谢朝海、毕马宁、陈雪秀。

引　言

依据国家信息安全等级保护管理规定制定本标准。

本标准是信息安全等级保护相关系列标准之一。

与本标准相关的系列标准包括：

——GB/T 22239—2008《信息系统安全等级保护基本要求》；

——国家标准《信息系统安全等级保护实施指南》；

——国家标准《信息系统安全等级保护测评准则》。

本标准依据等级保护相关管理文件，从信息系统所承载的业务在国家安全、经济建设、社会生活中的重要作用和业务对信息系统的依赖程度这两方面，提出确定信息系统安全保护等级的方法。

信息安全技术
信息系统安全等级保护定级指南

1 范围

本标准规定了信息系统安全等级保护的定级方法，适用于为信息系统安全等级保护的定级工作提供指导。

2 规范性引用文件

下列文件中的条款通过在本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8 信息技术 词汇 第8部分：安全 (GB/T 5271.8—2001，idt ISO/IEC 2382-8：1998)

GB 17859 计算机信息系统安全保护等级划分准则

3 术语和定义

GB/T 5271.8 和 GB 17859 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 security

信息安全等级保护工作直接作用的具体的信息和信息系统。

3.2

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。

3.3

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。

3.4

系统服务 system service

信息系统为支撑其所承载业务而提供的程序化过程。

4 定级原理

4.1 信息系统安全保护等级

根据等级保护相关管理文件，信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，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，信息系统受到破坏后，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，信息系统受到破坏后，会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，信息系统受到破坏后，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，信息系统受到破坏后，会对国家安全造成特别严重损害。

4.2 信息系统安全保护等级的定级要素

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度。

4.2.1 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。

4.2.2 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。

4.3 定级要素与等级的关系

定级要素与信息系统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	第二级
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

5 定级方法

5.1 定级的一般流程

信息系统安全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，信息系统定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信息系统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信息系统安全保护等级称系统服务安全保护等级。

确定信息系统安全保护等级的一般流程如下：

a） 确定作为定级对象的信息系统；

b） 确定业务信息安全受到破坏时所侵害的客体；

c） 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；

d） 依据表2，得到业务信息安全保护等级；

e） 确定系统服务安全受到破坏时所侵害的客体；

f） 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；

g） 依据表3，得到系统服务安全保护等级；

h) 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确定为定级对象的安全保护等级。

上述步骤如图1确定等级一般流程所示。

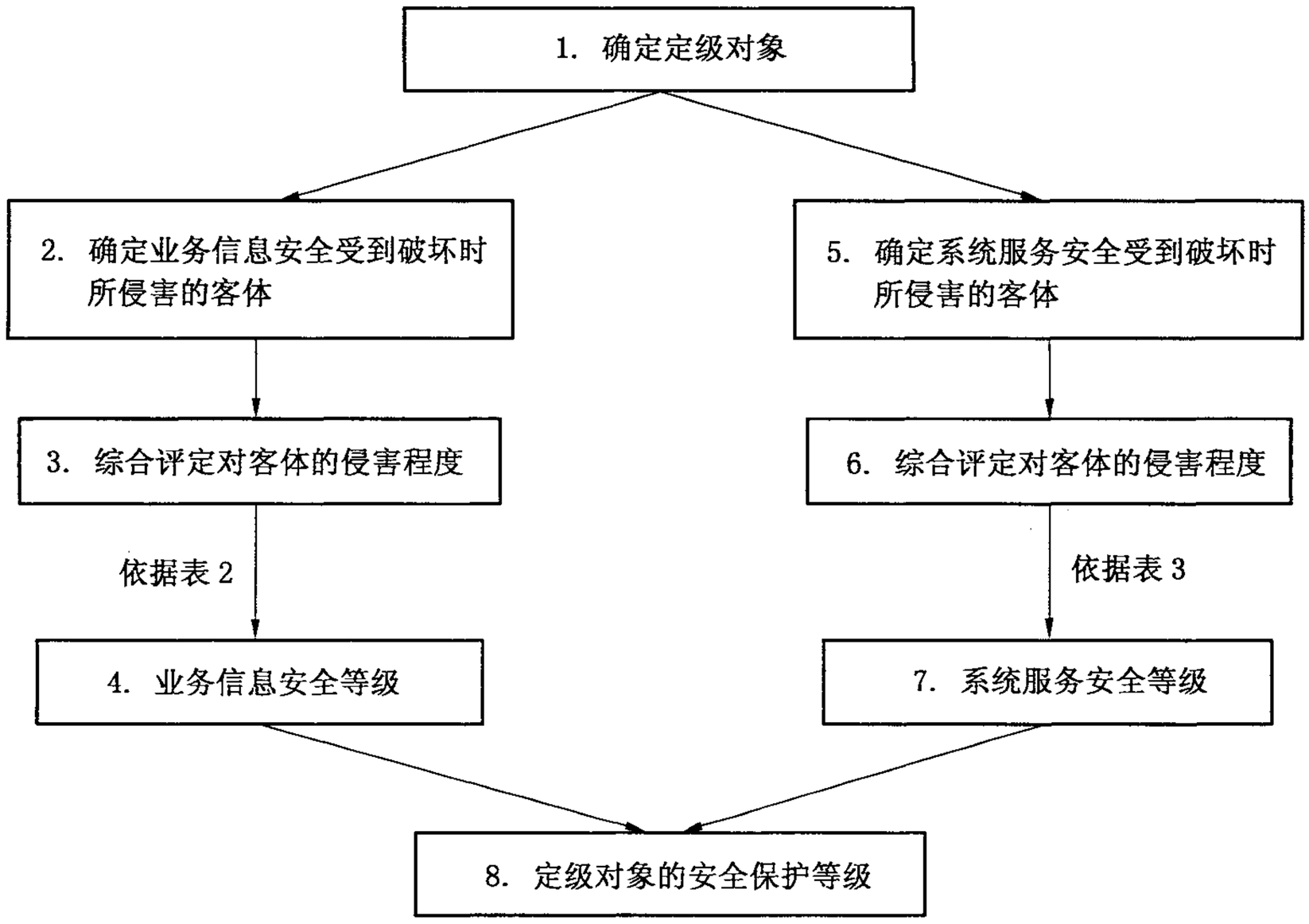

图1 确定等级一般流程

5.2 确定定级对象

一个单位内运行的信息系统可能比较庞大，为了体现重要部分重点保护，有效控制信息安全建设成本，优化信息安全资源配置的等级保护原则，可将较大的信息系统划分为若干个较小的、可能具有不同安全保护等级的定级对象。

作为定级对象的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) 具有信息系统的基本要素。作为定级对象的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有形实体。应避免将某个单一的系统组件，如服务器、终端、网络设备等作为定级对象。

c) 承载单一或相对独立的业务应用。定级对象承载“单一”的业务应用是指该业务应用的业务流程独立，且与其他业务应用没有数据交换，且独享所有信息处理设备。定级对象承载“相对独立”的业务应用是指其业务应用的主要业务流程独立，同时与其他业务应用有少量的数据交换，定级对象可能会与其他业务应用共享一些设备，尤其是网络传输设备。

5.3 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。

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。

影响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。

影响公民、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。

确定作为定级对象的信息系统受到破坏后所侵害的客体时，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。

各行业可根据本行业业务特点，分析各类信息和各类信息系统与国家安全、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关系，从而确定本行业各类信息和各类信息系统受到破坏时所侵害的客体。

5.4 确定对客体的侵害程度

5.4.1 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信息系统服务的破坏，其中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信息系统可以及时、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。

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。

5.4.2 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信息系统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。

不同危害后果的三种危害程度描述如下：

——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。

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。由于各行业信息系统所处理的信息种类和系统服务特点各不相同，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。

5.5 确定定级对象的安全保护等级

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	第二级
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	第二级
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

作为定级对象的信息系统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 等级变更

在信息系统的运行过程中，安全保护等级应随着信息系统所处理的信息和业务状态的变化进行适当的变更，尤其是当状态变化可能导致业务信息安全或系统服务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，可能影响到系统的安全保护等级时，应根据第5章给出的定级方法重新定级。