ICS 65.160
X 85
备案号：31590—2011

YC

中华人民共和国烟草行业标准

YC/T 389—2011

烟草行业信息系统安全等级保护与信息安全事件的定级准则

Classification criteria for classified security protection of information system and information security incident of tobacco industry

2011-03-25 发布　　2011-04-01 实施

国家烟草专卖局　发布

目　次

前　言

本标准按照 GB/T 1.1—2009《标准化工作导则　第1部分：标准的结构和编写》给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由国家烟草专卖局提出。

本标准由全国烟草标准化技术委员会信息分技术委员会(SAC/TC 144/SC 7)归口。

本标准起草单位：国家烟草专卖局烟草经济信息中心、中国标准化研究院。

本标准主要起草人：张雪峰、任冠华、高一军、耿刚勇、王海清、黄云海、耿欣、陈淑仪、魏宏。

烟草行业信息系统安全等级保护与信息安全事件的定级准则

1 范围

本标准规定了烟草行业信息系统安全等级保护(以下简称为安全等级保护)的等级划分和定级方法,烟草行业信息安全事件(以下简称为信息安全事件、事件)的分级、分类和定级,并给出了信息系统安全等级保护和信息安全事件的定级结果报告的格式。

本标准适用于烟草行业信息系统安全等级保护与信息安全事件的定级。

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/Z 20986—2007 信息安全技术 信息安全事件分类分级指南

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

关于信息安全等级保护工作的实施意见(公通字[2004]66号)

信息安全等级保护管理办法(公通字[2007]43号)

关于开展全国重要信息系统安全等级保护定级工作的通知(公信安[2007]861号)

3 术语和定义

GB/T 5271.8—2001、GB/T 20269—2006、GB/T 20271—2006、GB/T 20274.1—2006、GB/T 20275—2006确立的以及下列术语和定义适用于本文件。

3.1

信息系统 information system

基于计算机或计算机网络,按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索和服务的人机系统。

3.2

信息系统安全 security of information system

信息系统及其存储、传输和处理的信息的保密性、完整性和可用性的表征。

[GB/T 20271—2006,定义3.1.1]

3.3

信息系统安全等级保护 classified security protection of information system

对信息系统分等级实施安全保护和等级化管理。

3.4

保密性;机密性 confidentiality

数据所具有的特性,即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

[GB/T 5271.8—2001,定义8.1.9]

3.5

完整性 integrity

包括数据完整性和系统完整性。数据完整性表征数据所具有的特性，即无论数据形式作何变化，数据的准确性和一致性均保持不变的程度。系统完整性表征系统在防止非授权用户修改或使用资源和防止授权用户不正确地修改或使用资源的情况下，系统能履行其操作目的的品质。

[GB/T 20269—2006，定义 3.1]

3.6

可用性 availability

表征数据或系统根据授权实体的请求可被访问与使用程度的安全属性。

[GB/T 20269—2006，定义 3.2]

3.7

业务子系统 business subsystem

由信息系统的一部分组件构成，是信息系统中能够承载某项业务工作的子系统。

3.8

事件 incident

信息系统中试图改变目标状态，并造成或可能造成损害的行为。

[GB/T 20275—2006，定义 3.1]

3.9

信息安全事件 information security incident

由单个或一系列意外或有害的信息安全异常现象所组成，极有可能危害业务运行和威胁信息安全。

3.10

泄露 disclosure

计算机安全的违规，使数据被未经授权的实体使用。

[GB/T 5271.8—2001，定义 8.5.15]

3.11

威胁 threat

能够通过未授权访问、毁坏、揭露、数据修改和/或拒绝服务对系统造成潜在危害的任何环境或事件。

[GB/T 20274.1—2006，定义 3.1.27]

3.12

恢复时间目标 recovery time objective

故障发生后，信息系统或业务功能从停顿到必须恢复的时间要求。

4 信息系统安全等级保护

4.1 概述

信息系统安全等级保护的定级准则是实施信息系统安全保障的前提和基础，本标准结合烟草行业自身的信息系统特点，给出了烟草行业信息系统安全等级保护的等级划分和定级方法。

4.2 等级划分

根据烟草行业信息系统的重要程度，以及信息系统遭到破坏后，对国家安全、烟草业务的影响程度以及所造成的经济损失大小，将烟草行业信息系统安全保护等级由低到高依次划分为自主保护级、指导保护级、监督保护级、强制保护级和专控保护级五个安全等级。烟草行业信息系统安全等级保护的划分

见表1。

表1 信息系统安全等级保护划分

等级	名称	描 述
第一级	自主保护级	主要对象为一般的信息系统。信息系统遭到破坏后，对烟草业务造成局部性影响且经济损失程度一般，由信息系统建设和使用单位按本单位信息化工作部门有关规定进行自行保护，它需要实施系统安全运行所需的基本的技术要求和安全管理要求
第二级	指导保护级	主要对象为较重要的信息系统。信息系统遭到破坏后，对烟草业务造成区域性影响且经济损失程度较大，由信息系统建设和使用单位在国家烟草专卖局有关部门的指导下进行保护，它需要实施系统安全运行所需的一定程度的技术要求和安全管理要求
第三级	监督保护级	主要对象为重要的信息系统。信息系统遭到破坏后，对烟草业务造成全局性影响或经济损失程度严重，由信息系统建设和使用单位在国家烟草专卖局有关部门的监督下进行保护，它需要实施系统安全运行所需的高程度的技术要求和严格的安全管理要求
第四级	强制保护级	主要对象为涉密信息系统。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。信息系统建设和使用单位应依据国家有关管理规范、技术标准和业务专门需求进行保护。国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查
第五级	专控保护级	主要对象为涉及国家安全的信息系统。信息系统受到破坏后，会对国家安全造成特别严重损害。信息系统建设和使用单位应依据国家管理规范、技术标准和业务特殊安全需求进行保护。国家指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查

注：对第四级的涉密信息系统和第五级国家安全的信息系统应按照国家保密工作部门有关涉密信息系统分级保护的管理规定和BMB17-2006技术标准进行保护，其内容不在本标准范围内。信息系统保护等级实施包括技术和管理要求。其中技术部分包括物理安全、网络安全、主机安全、应用安全和数据安全及备份恢复等，管理部分包括：安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理等。在信息系统建设过程中，使用单位可参照GB/T 20270—2006、GB/T 20271—2006、GB/T 20272—2006、GB/T 20273—2006、GA/T 671—2006等技术标准以及GB/T 20269—2006、GB/T 20282—2006、GB/T 22239—2008、《信息系统等级保护安全设计技术要求》(信安秘字[2009]059号)等管理标准同步建设符合该等级要求的信息安全设施。信息系统保护等级实施的内容，不在本标准的范围内。

4.2.1 信息系统重要程度

信息系统安全等级是信息系统重要程度的表征。烟草行业信息系统安全等级保护所对应的信息系统重要程度为：

——第一级为一般的信息系统；

——第二级为较重要的信息系统；

——第三级为重要的信息系统；

——第四级为涉密信息系统；

——第五级为涉及国家安全的信息系统。

4.2.2 信息系统服务范围

烟草行业信息系统的服务范围可用局部性、区域性和全局性影响来判定，其中：

——局部性影响：系统遭到破坏后，只对直属单位以下（地市级公司、卷烟厂和生产点），国家烟草专卖局（以下简称国家局）直属单位机关内部和国家局机关内部范围内的业务工作造成影响，不涉及其他单位或国家局对所属单位的管理工作；

——区域性影响：系统遭到破坏后，对国家局直属单位范围内的业务工作造成影响，不涉及与其他国家局直属单位有关联的各项工作；

——全局性影响：系统遭到破坏后，对国家局进行行业管理工作或国家局直属单位之间的相互关联工作造成影响；或因信息失密给全行业范围的业务和管理工作带来较大影响或造成社会不良影响。

4.2.3 经济损失

信息系统遭到破坏后对烟草行业业务所造成的经济损失，可用信息系统的资产损失大小来判定。

信息系统是由硬件、软件和系统所承载的信息及人员等组成。信息系统的资产价值主要包含但不限于以下内容：

a) 硬件资产（例如，服务器设备、客户端设备、打印机及存储器等外围设备）；

b) 软件资产（例如，系统软件、应用软件、开发工具和实用程序等）；

c) 信息资产（例如，系统数据、业务数据、系统文档和技术资料等）；

d) 生产能力或提供服务能力（例如，系统对于烟草业务运作的支撑程度、系统对于其他系统的影响程度以及系统涉及到的用户数量等）；

e) 人员（与信息系统运营有关的技术和管理人员等）；

f) 无形资产（例如，信誉、形象等）。

其中系统软件、应用软件、系统数据、业务数据和技术资料的含义，如下：

1) 系统软件：操作系统软件、数据库系统软件和应用管理软件；

2) 应用软件：电子政务系统、电子商务系统、卷烟生产经营决策管理系统、生产与仓库管理系统、生产执行系统、生产线与仓库管理系统及其支持软件应用系统运行的程序等；

3) 系统数据：包括数据字典、权限设置、存储分配、网络地址、网管参数、硬件配置及其他系统配置参数等；

4) 业务数据：包括统计、销售、生产、财务、烟叶、专卖等与行业生产、经营、管理有关的基础数据及其他相关数据等；

5) 技术资料：与信息系统有关的技术文件、图表、程序与数据等。

注：网络设施的资产价值另作处理，不包含在本标准的资产价值中。

信息系统建设和使用单位应按上述资产价值所包含的内容，计算信息系统的经济损失。经济损失与损害程度关系见表2。

表2 经济损失与损害程度关系

损害程度	经济损失（人民币：万元）
一般损害	≥50 且＜100
较大损害	≥100 且＜300
严重损害	≥300

4.3 定级方法

4.3.1 定级要素

信息安全是保证信息的保密性、完整性和可用性。

信息系统安全保护包括信息系统的安全运行控制和对运行中的信息系统所存储、传输和处理的信息的安全保护。信息系统安全包括业务信息安全和系统服务安全，信息系统安全保护等级的定级要素为：

——业务信息安全定级要素：反映信息系统的业务信息安全，确保信息系统内信息的保密性、完整性和可用性。它关注的是保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改。根据业务信息安全被破坏时所侵害的业务信息类型以及对相应系统的侵害程度来确定；

——系统服务安全定级要素：反映信息系统的业务服务保证性的程度，即系统提供业务连续性的程度。它关注的是保护系统连续正常的运行，避免因对系统的未授权修改、破坏而导致系统不可用。根据系统服务安全被破坏时所侵害的系统服务范围以及对相应系统的侵害程度来确定。

4.3.2 定级流程

信息系统定级过程包括系统划分、等级确定和定级结果报告三个阶段：

a) 系统划分：按4.3.3要求，划分系统并确定需要定级信息系统；

b) 等级确定：按4.3.4要求，首先确定业务信息安全保护等级要素和系统服务安全保护等级要素，然后确定信息系统的安全保护等级；

c) 定级结果报告：按4.3.5的要求，信息系统建设和使用单位将信息系统安全等级保护的定级结果，上报国家局审核(审批)与备案。

4.3.3 系统划分

烟草行业应用信息系统的划分可参照YC/Z 204—2006表A.8烟草行业应用系统标准明细表，主要包括电子政务应用系统、电子商务应用系统和卷烟生产经营决策管理系统等。根据烟草行业信息系统的重要程度和业务对信息系统的依赖度进行综合分析后，确定需要定级信息系统。

若需定级的信息系统复杂，则可根据信息系统承载的多项业务类型、提供的服务范围等方式，将系统划分为若干业务子系统。子系统是定级划分的最小单元。

示例："烟草行业办公自动化管理系统"可划分为直属单位或直属单位以下的办公自动化管理系统子系统。

信息系统划分后，应有每个信息系统(子系统)的基本情况描述，其描述文件应包含但不限于以下内容：

——系统(子系统)的名称和概述；

——系统提供的业务信息类型；

——系统(子系统)应用的服务范围；

——系统恢复时间目标值。

4.3.4 等级确定

4.3.4.1 确定业务信息安全保护等级

4.3.4.1.1 业务信息类型

信息类型反映了信息资产在信息系统中的保护程度，是划分等级时的重要依据。烟草行业信息系统承载的业务信息类型可划分为：

——公开信息：信息系统中对社会公众开放的信息，例如提供许可证申办的各种服务信息，包括申请表的下载或网上填写，许可证的申办情况查询，许可证受理、办理公告，许可证申办指南，人员招聘信息，相关法律、法规和政策性文件检索等信息；

——内部信息：信息系统中具有烟草行业内部使用的一般价值或需要进行一定保密程度的信息，例

如用于国家局和直属单位核发许可证的内部审批，许可证办理数据的统计，零售许可证管理数据的上传汇总，申办流程控制与申办人员权限控制等信息；

——重要信息：信息系统中具有内部使用的重要价值或需要进行严格保密程度的信息，例如涉及行业政策、计划、人事信息、财务信息，行业生产经营中的重要数据信息及各单位自有自用的不适宜在行业传播的数据信息。

若信息系统内包含多种信息类型时，原则上可选择较高信息的业务信息类型。

注：本标准所规定的信息类型只涉及工作秘密和商业秘密，不包括国家秘密信息。

4.3.4.1.2 对系统的侵害程度

业务信息安全被破坏时对相应系统的侵害程度可用一般损害、较大损害和严重损害来判定。经济损失与损害程度关系可参见表2。

4.3.4.1.3 业务信息安全保护等级

根据业务信息安全被破坏时所侵害的业务信息类型以及对相应系统的侵害程度来确定业务信息安全保护等级。按表3所示的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3 业务信息安全保护等级矩阵表

破坏时所侵害的业务信息类型	对相应系统的侵害程度		
	一般损害	较大损害	严重损害
公开信息	第一级	第一级	第一级
内部信息	第一级	第二级	第二级
重要信息	第二级	第二级	第三级

4.3.4.2 确定系统服务安全保护等级

4.3.4.2.1 信息系统服务范围

烟草行业信息系统的服务范围用4.2.2定义的局部性、区域性和全局性来判定。

4.3.4.2.2 对系统的侵害程度

系统服务安全被破坏时对相应系统的侵害程度用下列三种危害程度来判定：

——一般损害：系统具有基本的数据备份功能，在遭到破坏后能够不限时的恢复部分系统功能，对烟草行业业务影响较小且经济损失较少；

——较大损害：系统具有一定的数据备份功能，在遭到破坏后能够在一段时间内（恢复时间目标值在4 h～8 h内）恢复绝大部分功能，对影响烟草行业业务影响较大且经济损失较大；

——严重损害：系统具有较高的数据备份和系统备份功能，在遭到破坏后能够较快的（恢复时间目标值<4 h内）恢复所有部分功能，对影响烟草行业业务影响重大且经济损失严重。

注：恢复能力是以故障发生后信息系统或业务功能能够在一定时间内恢复原有状态的能力，可从恢复时间和恢复程度上来衡量。恢复时间越短、恢复程度越接近系统正常运行状态，表明恢复能力越高。

4.3.4.2.3 系统服务安全保护等级

根据安全被破坏时所侵害的系统服务范围以及对相应系统的侵害程度来确定系统服务安全保护等级。按表4所示的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 4　系统服务安全保护等级矩阵表

破坏时所侵害的系统服务范围	对相应系统的侵害程度		
	一般损害	较大损害	严重损害
局部范围	第一级	第一级	第一级
区域范围	第一级	第二级	第二级
全行业范围	第二级	第二级	第三级

4.3.4.3　等级确定

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确定为定级对象的安全保护等级。

对具有子系统的信息系统的安全等级确定分为两个步骤，首先将信息系统划分为若干子系统并分别确定每个子系统的安全等级保护，然后根据信息系统内各子系统的最高等级来确定整体信息系统的安全等级保护。

若确定信息系统（子系统）安全等级的业务信息安全保护等级要素或系统服务安全保护等级要素发生变化时（例如系统主要承载的业务信息类型发生变化，或系统服务范围发生变化，或对系统的业务影响程度发生变化），则应重新确定系统安全等级保护。

4.3.5　定级结果报告

烟草行业信息安全等级保护工作按照“谁主管谁负责、谁运营谁负责”的要求，由信息系统建设和使用单位落实等级保护措施。

对信息系统保护等级评定为第一级的信息系统，由信息系统建设和使用单位按本单位信息化工作部门有关规定进行自行保护。

对信息系统保护等级评定为第二级的信息系统，由信息系统建设和使用单位在国家烟草专卖局有关部门的指导下进行保护，并按附录 A 的要求上报国家局审核与备案。

对信息系统保护等级评定为第三级的重要信息系统，由信息系统建设和使用单位在国家烟草专卖局有关部门的监督下进行保护，并按附录 A 的要求上报国家局审批与备案。

对确定为第四级和第五级的信息系统应按公信安〔2007〕861 号文件和国家保密局有关的规定，进行评审、审批和备案。

5　信息安全事件

5.1　概述

为对烟草行业突发的信息安全事件作出快速、有效的处置，需确定烟草行业信息安全事件的定级准则，它是实施应急处理的前提和基础。本标准从信息安全事件的事件分级、分类和定级三个方面进行了描述。

烟草行业信息安全事件的分级参照了国务院发布《国家突发公共事件总体应急预案》对突发公共事件由高到低划分的原则，按突发信息安全事件对信息系统和烟草业务的损失或破坏的程度进行分级划分。

信息系统面临多种威胁，可能面临自然、环境和技术故障等非人为因素的威胁，也可能面临人员失误和恶意攻击等人为因素的威胁。为便于判定和处置突发的信息安全事件，本标准按信息安全事件发生的性质对信息安全事件进行分类。

事件定级规定了发生重大或较大信息安全事件的单位向烟草经济信息中心上报的步骤，以及发生信息安全事件后进行综合定级方法。

5.2 事件分级

5.2.1 级别划分

烟草行业信息安全事件按突发信息事件对信息系统和烟草业务影响的程度和影响范围等因素，划分为特别重大事件（Ⅰ级）、重大事件（Ⅱ级）、较大事件（Ⅲ级）和一般事件（Ⅳ级），其中：

——特别重大事件（Ⅰ级）：导致信息系统和烟草业务有特别严重的损失或破坏的信息安全事件；

——重大事件（Ⅱ级）：导致重大或破坏的信息安全事件；

——较大事件（Ⅲ级）：导致信息系统和烟草业务有较大的损失或破坏的信息安全事件；

——一般事件（Ⅳ级）：导致信息系统和烟草业务有一定的损失或破坏的信息安全事件。

烟草行业信息安全事件分级划分见表5。

表5 信息安全事件的分级划分

级别	描　述
Ⅰ级	特别重大事件。信息安全事件导致信息系统和烟草业务遭受特别严重的损失或破坏，即突发信息安全事件造成系统大面积瘫痪，恢复系统正常运行所需付出的代价十分巨大；或信息系统丧失业务处理能力，使烟草行业的全局性业务处理能力受到特别重大影响；或特别重要信息的失窃或泄密，消除安全事件负面影响所需付出的代价特别巨大
Ⅱ级	重大事件。信息安全事件导致信息系统和烟草业务有重大的损失或破坏，即突发信息安全事件造成系统长时间中断或系统大面积瘫痪，恢复时间目标值超过8 h；或信息系统无法提供服务或无法提供有效服务，使烟草行业的全局性业务处理能力受到重大影响；或重要信息的失窃或泄密，消除安全事件负面影响所需付出的代价巨大
Ⅲ级	较大事件。信息安全事件导致信息系统和烟草业务有较大的损失或破坏，即突发信息安全事件造成系统较长时间中断或局部瘫痪，恢复时间目标值在4 h～8 h内；或信息系统无法提供服务或无法提供有效服务，使烟草行业的全局性业务处理能力受到较大影响或区域性业务处理能力受到重大影响；或内部信息的失窃或泄密，消除安全事件负面影响所需付出的代价较大
Ⅳ级	一般事件。信息安全事件导致信息系统和烟草业务有一定的损失或破坏，即突发信息安全事件造成系统中断影响系统效率，恢复时间目标值小于4 h；或信息系统无法提供服务或无法提供有效服务，使烟草行业的区域性或局部性业务处理能力受到影响；或信息的失窃或泄密，消除安全事件负面影响所需付出一定的代价
注：对不同安全等级保护的烟草行业应用信息系统，恢复时间目标值可参考上述参数作适当的调整。	

5.2.2 分级要素

信息安全事件分级要素为信息系统重要程度、业务影响和资产损失，其中：

a) 信息系统重要程度：根据信息系统所要实现的业务目标以及信息系统所拥有信息资产而定的要素；

b) 业务影响：衡量信息系统无法提供服务或无法提供有效服务，对业务服务保证性影响程度的要素；

c) 资产损失：衡量恢复系统正常运行或消除安全事件负面影响所需付出资产代价的要素。

5.2.2.1 系统重要程度

将烟草行业信息系统分为重要、较重要和一般的信息系统，与4.2中所给出的安全等级保护所划分系统相对应。其中：

——特别重要的信息系统，对应于信息系统安全等级保护中的第四级系统；

——重要的信息系统，对应于信息系统安全等级保护中的第三级系统；

——较重要的信息系统，对应于信息系统安全等级保护中的第二级系统；

——一般的信息系统，对应于信息系统安全等级保护中的第一级系统。

信息系统重要程度的级别赋值见表6。

表6 信息系统重要程度的级别赋值

级别赋值	信息系统重要程度
第四级	特别重要的信息系统
第三级	重要的信息系统
第二级	较重要的信息系统
第一级	一般的信息系统

5.2.2.2 业务影响

业务影响是评定突发信息安全事件的一个重要要素。按突发信息安全事件造成信息系统无法提供服务或无法提供有效服务，对烟草业务影响程度加以赋值。业务影响的级别赋值见表7。

表7 业务影响的级别赋值

级别赋值	描　述
Ⅰ级	突发信息安全事件造成信息系统丧失业务处理能力，使烟草行业的全局性业务处理能力受到特别重大影响；或系统大面积瘫痪，恢复系统正常运行所需付出的代价十分巨大；或特别重要信息的失窃或泄密，消除安全事件负面影响所需付出的代价特别巨大
Ⅱ级	突发信息安全事件造成信息系统无法提供服务或无法提供有效服务，使烟草行业的全局性业务处理能力受到重大影响；或系统大面积瘫痪，恢复时间目标值超过8 h
Ⅲ级	突发信息安全事件造成信息系统无法提供服务或无法提供有效服务，使烟草行业的全局性业务处理能力受到较大影响或区域性业务处理能力受到重大影响；或系统长时间中断或局部瘫痪，恢复时间目标值在4 h～8 h内
Ⅳ级	突发信息安全事件造成信息系统无法提供服务或无法提供有效服务，使烟草行业的区域性或局部性业务处理能力受到一定的影响；或系统中断影响系统效率，恢复时间目标值小于4 h
注：对不同安全等级保护的烟草行业应用信息系统，恢复时间目标值可参考上述参数作适当的调整。	

5.2.2.3 资产损失

资产损失是指由于突发信息安全事件所导致资产损失，即恢复系统正常运行和消除安全事件负面影响所需付出的经济损失。资产损失的级别赋值见表8。

表 8 资产损失的级别赋值

级别赋值	资产损失(人民币:万元)
Ⅰ级	≥500
Ⅱ级	≥300,且<500
Ⅲ级	≥100,且<300
Ⅳ级	≥50,且<100

5.3 事件分类

5.3.1 概述

本标准按信息安全事件发生的性质,将信息安全事件分为自然灾害、设施故障、系统异常和其他事件四大类;在四大类的基础上,又细分为若干个分类。信息安全事件的分类见表 9。

表 9 信息安全事件的分类

大类	分 类
自然灾害	火灾或水患
	气象灾害
	地震灾害
	地质灾害
	其他自然灾害
设施故障	软硬件自身故障
	外围设施故障
	人为破坏事故
系统异常	有害程序事件
	网络攻击事件
	信息破坏事件
	信息内容事件
其他事件	不能归为以上类别的信息安全事件

5.3.2 自然灾害事件

自然灾害事件是指由于不可抗拒的自然灾害对信息系统造成物理破坏而导致的信息安全事件。它可分为火灾和水患、气象灾害、地震灾害、地质灾害以及其他自然灾害等。

5.3.3 设施故障事件

由于保障信息系统正常运行所需的设施出现故障而导致的信息安全事件。可分为软硬件自身故障、外围设施故障、人为破坏事故和其他设施故障的事件,其中:

——软硬件自身故障事件:因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的信息安全事件;

——外围设施故障事件：由于保障信息系统正常运行所必须的外部设施出现故障而导致的信息安全事件，例如电力故障、线路故障及其他外围保障设施故障等导致的信息安全事件；

——人为破坏事故事件：人为蓄意对保障信息系统正常运行的软硬件等实施窃取、破坏造成的信息安全事件；或由于人为的遗失、误操作以及其他无意行为造成信息系统软硬件等遭到破坏，影响信息系统正常运行的信息安全事件；

——其他设施故障事件：不能包含上述分类中的设施故障事件。

5.3.4 系统异常事件

通过网络或其他手段，对信息系统实施攻击而导致的信息安全事件。可分为有害程序事件、网络攻击事件、信息破坏事件和信息内容安全事件等。

5.3.4.1 有害程序事件

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信息安全事件。包括计算机病毒事件、蠕虫事件、木马事件、流氓软件和其他有害程序事件等，其中：

——计算机病毒事件：蓄意制造、传播计算机病毒，或是因受到计算机病毒影响而导致的信息安全事件；

——蠕虫事件：蓄意制造、传播蠕虫，或是因受到蠕虫影响而导致的信息安全事件；

——木马事件：蓄意制造、传播木马程序，或是因受到木马程序影响而导致的信息安全事件；

——流氓软件事件：在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵犯用户合法权益的信息安全事件；

——其他有害程序事件：不能包含上述分类中的有害程序事件。

5.3.4.2 网络攻击事件

通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷和程序缺陷等对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件和其他网络攻击事件等，其中：

——拒绝服务攻击事件：利用信息系统缺陷或通过攻击的手段，以大量消耗信息系统的CPU、内存、磁盘空间或网络带宽等资源，从而影响信息系统正常运行为目的信息安全事件；

——后门攻击事件：利用软件系统、硬件系统设计过程中留下的后门或有害程序所设置的后门而对信息系统实施的攻击的信息安全事件；

——漏洞攻击事件：除拒绝服务攻击事件和后门攻击事件之外，利用信息系统配置缺陷、协议缺陷、程序缺陷等漏洞，对信息系统实施攻击的信息安全事件；

——网络扫描窃听事件：利用网络扫描或窃听软件，获取信息系统网络配置、端口和服务等特征而导致的信息安全事件；

——其他网络攻击事件：不能包含上述分类中的网络攻击事件。

5.3.4.3 信息破坏事件

通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏和窃取等而导致的信息安全事件。包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其他信息破坏事件等，其中：

——信息篡改事件：未经授权将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件，例如网页篡改等导致的信息安全事件；

——信息假冒事件：通过假冒他人信息系统收发信息而导致的信息安全事件，例如网页假冒等导致

的信息安全事件；

——信息泄漏事件：因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者而导致的信息安全事件；

——信息窃取事件：未经授权用户利用可能的技术手段恶意主动获取信息系统中信息而导致的信息安全事件；

——信息丢失事件：因误操作、人为蓄意或软硬件缺陷等因素导致信息系统中的信息丢失而导致的信息安全事件；

——其他信息破坏事件：不能包含上述分类中的信息破坏事件。

5.3.4.4 信息内容事件

通过网络方式传播异常信息的信息安全事件。

示例：通过垃圾邮件传播异常信息的信息内容安全事件。

5.3.5 其他信息安全事件

不能归为以上类别的信息安全事件。

5.4 事件定级

5.4.1 概述

为快速、有效地处置相应的安全事件，并对已发生的信息安全事件进行评估和总结，本标准建议对信息系统中发生的信息安全事件按先期处置与后期处置两个阶段进行综合定级，对可能涉及国家秘密的重大失密、泄密事件，应按国家烟草专卖局保密委员会的相关规定执行，不在本标准的范围内。

5.4.2 先期处置与初步定级

先期处置与初步定级的步骤如下：

a) 在信息安全事件发生后，发生信息安全事件的单位应分析和鉴定信息事件产生的原因，保存所有的文件和记录的相关证据；

b) 按表6～表8的要求，对系统重要程度、业务影响和资产损失分级要素的级别赋值；

c) 用分级要素中的最高级别赋值作为信息安全事件的初步确定级别；

d) 发生重大或较大信息安全事件的单位应按附录B规定的步骤和时限及时向国家局烟草经济信息中心报告，上报信息安全事件的步骤见附录B，信息安全事件的上报表见表B.1。

注：信息安全事件应急预案是针对安全事件级别制定相应的处置方案及应采取的措施，其内容不在本标准的范围内。

5.4.3 后期处置与最终定级

发生重大或较大信息安全事件的单位，在信息安全事件处理后应有相应的反馈程序。根据事件的性质和造成的实际影响进行总结和评估，作为该事件的最终综合定级结果；并将信息安全事件的处理结果，按表B.2所示的要求，报国家局烟草经济信息中心备案。

附 录 A
（规范性附录）
信息系统安全等级保护的定级结果报告

对安全等级保护确定为第二级或第三级的信息系统，信息系统建设和使用单位应将信息系统安全等级保护的定级结果，上报国家局审核（审批）与备案。审核（审批）与备案的步骤为：

a) 信息系统建设和使用单位将自行确定的信息系统的安全等级保护的定级结果，按表 A.1 要求填写信息系统安全等级保护的审核（审批）表，上报国家局审核（审批）；

b) 国家局审核（审批）信息系统建设和使用单位上报的信息系统安全等级保护的审核（审批）表，并对安全等级保护加以确认后，信息系统建设和使用单位按表 A.1 要求填写信息系统安全等级保护的定级备案表，报国家局备案；

c) 已确定安全等级保护并已备案的系统，如果进行改扩建，则需依据 4.3.4 的定级步骤，重新确定系统的安全等级保护，并应在自变更之日三十日内，将变更情况按上述步骤报国家局审核（审批）与备案。

表 A.1 信息系统安全等级保护的定级审核(审批)与备案表

<table>
<tr><td colspan="6">单位基本情况</td></tr>
<tr><td>单位名称</td><td colspan="5"></td></tr>
<tr><td>单位地址</td><td colspan="5"></td></tr>
<tr><td rowspan="3">报告人情况</td><td>姓名</td><td></td><td>所在部门</td><td colspan="2"></td></tr>
<tr><td>电话</td><td></td><td>传真</td><td colspan="2"></td></tr>
<tr><td>电子邮件</td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="6">系统(子系统)基本情况</td></tr>
<tr><td>系统名称</td><td colspan="2"></td><td>子系统名称</td><td colspan="2"></td></tr>
<tr><td>系统服务范围</td><td colspan="2">□全行业 □区域 □局部</td><td>子系统服务范围</td><td colspan="2">□区域 □局部</td></tr>
<tr><td>业务信息类型</td><td colspan="5">□重要信息 □内部信息 □公开信息</td></tr>
<tr><td>系统侵害程度</td><td colspan="5">□严重 □较大 □一般</td></tr>
<tr><td colspan="6">定级基本情况</td></tr>
<tr><td>定级说明</td><td colspan="2">□初次定级 □重新定级</td><td>确定等级</td><td colspan="2"></td></tr>
<tr><td>定级时间</td><td colspan="2">年 月 日</td><td>主管签字</td><td colspan="2"></td></tr>
<tr><td>附件清单</td><td colspan="5"></td></tr>
<tr><td colspan="6">以下由负责审核(审批)的主管部门填写</td></tr>
<tr><td>备案号</td><td colspan="5">No.</td></tr>
<tr><td>备案时间</td><td colspan="2">年 月 日</td><td>备案经手人</td><td colspan="2"></td></tr>
<tr><td>主管部门
备案(审查)意见</td><td colspan="5">(盖章)
年 月 日</td></tr>
<tr><td>备注</td><td colspan="5"></td></tr>
</table>

【填表说明】

1. 用户在选择处请在内划“√”;
2. 本表中位置不够填写的地方,可另附页说明。

附 录 B
（规范性附录）
信息安全事件的定级结果报告

发生重大或较大信息安全事件的单位应将信息安全事件情况上报烟草经济信息中心，其步骤为：

a) 为保证上报信息安全事件的及时性和准确性，在安全事件的先期处置阶段，应立即向国家局烟草经济信息中心口头报告，并按 5.4.2 的要求填写表 B.1 的信息安全事件上报表；

b) 为评估和总结已发生的信息安全事件，在安全事件的后期处置阶段，按 5.4.3 的要求填写表 B.2 的信息安全事件处理结果报告表，并在总结和评估后的 10 天内将评估报告上报国家局烟草经济信息中心备案。

表 B.1 信息安全事件的上报表

<table>
<tr><td colspan="7">单位基本情况</td></tr>
<tr><td>单位名称</td><td colspan="6"></td></tr>
<tr><td>单位地址</td><td colspan="6"></td></tr>
<tr><td rowspan="3">报告人情况</td><td>姓名</td><td colspan="2"></td><td>所在部门</td><td colspan="2"></td></tr>
<tr><td>电话</td><td colspan="2"></td><td>传真</td><td colspan="2"></td></tr>
<tr><td>电子邮件</td><td colspan="5"></td></tr>
<tr><td colspan="7">信息安全事件的简要描述</td></tr>
<tr><td>系统名称</td><td colspan="2"></td><td>子系统名称</td><td colspan="3"></td></tr>
<tr><td>事件发生的日期和时间、地点</td><td>日期和时间</td><td colspan="2">年 月 日 时</td><td>地点</td><td colspan="2"></td></tr>
<tr><td>事件后果</td><td colspan="6">□业务中断 □系统破坏 □数据丢失 □其他</td></tr>
<tr><td>影响范围</td><td colspan="6">□全局 □区域 □局部</td></tr>
<tr><td>事件是否结束</td><td colspan="6">□是 □否</td></tr>
<tr><td>事件持续时间</td><td colspan="6">□>8 h □4 h～8 h □<4 h</td></tr>
<tr><td colspan="7">定级基本情况</td></tr>
<tr><td rowspan="4">初步判定的事件类别</td><td>□自然灾害</td><td colspan="5">□ 火灾 □ 水灾 □ 气象灾害 □地震灾害 □地质灾害 □其他</td></tr>
<tr><td>□设施故障</td><td colspan="5">□ 硬软件故障 □外围设施故障 □人为破坏故障</td></tr>
<tr><td>□系统异常</td><td colspan="5">□有害程序事件 □网络攻击事件 □信息破坏事件
□内容异常</td></tr>
<tr><td>□其他事件</td><td colspan="5"></td></tr>
<tr><td rowspan="5">初步确定的事件等级</td><td rowspan="3">分级要素定级</td><td>系统重要程度</td><td colspan="4">□ Ⅰ级 □ Ⅱ级 □ Ⅲ级 □Ⅳ级</td></tr>
<tr><td>业务影响</td><td colspan="4">□ Ⅰ级 □ Ⅱ级 □ Ⅲ级 □Ⅳ级</td></tr>
<tr><td>资产损失</td><td colspan="4">□ Ⅰ级 □ Ⅱ级 □ Ⅲ级 □Ⅳ级</td></tr>
<tr><td colspan="2">综合定级</td><td colspan="4">□ Ⅰ级 □ Ⅱ级 □ Ⅲ级 □Ⅳ级</td></tr>
<tr><td>采取的措施</td><td colspan="6"></td></tr>
<tr><td>备注</td><td colspan="6"></td></tr>
<tr><td>单位审查意见</td><td colspan="6">（盖章）
年 月 日</td></tr>
</table>

【填表说明】

1. 用户在选择处请在内划“√”；
2. 本表中位置不够填写的地方，可另附页说明。

表 B.2　信息安全事件的处理结果报告表

<table>
<tr><td colspan="7">单位基本情况</td></tr>
<tr><td>单位名称</td><td colspan="6"></td></tr>
<tr><td>单位地址</td><td colspan="6"></td></tr>
<tr><td rowspan="3">报告人情况</td><td>姓名</td><td colspan="2"></td><td>所在部门</td><td colspan="2"></td></tr>
<tr><td>电话</td><td colspan="2"></td><td>传真</td><td colspan="2"></td></tr>
<tr><td>电子邮件</td><td colspan="5"></td></tr>
<tr><td colspan="7">信息安全事件的简要描述</td></tr>
<tr><td>系统名称</td><td colspan="3"></td><td>子系统名称</td><td colspan="2"></td></tr>
<tr><td>事件发生时间、地点</td><td>时间</td><td colspan="2">年　月　日　时</td><td>地点</td><td colspan="2"></td></tr>
<tr><td>事件后果</td><td colspan="6">□业务中断　□系统破坏　□数据丢失　□其他</td></tr>
<tr><td>影响范围</td><td colspan="6">□全局　□区域　□局部</td></tr>
<tr><td>恢复时间目标</td><td colspan="6">□>8 h　□4 h～8 h　□<4 h</td></tr>
<tr><td colspan="7">定级基本情况</td></tr>
<tr><td rowspan="4">事件类别</td><td>□自然灾害</td><td colspan="5">□ 火灾 □ 水灾 □ 气象灾害 □地震灾害 □地质灾害 □其他</td></tr>
<tr><td>□设施故障</td><td colspan="5">□ 硬软件故障　□外围设施故障　□人为破坏故障</td></tr>
<tr><td>□系统异常</td><td colspan="5">□有害程序事件　□网络攻击事件　□信息破坏事件
□内容异常</td></tr>
<tr><td>□ 其他事件</td><td colspan="5"></td></tr>
<tr><td rowspan="4">事件定级</td><td rowspan="3">分级要素定级</td><td>系统重要程度</td><td colspan="4">□ Ⅰ级　□ Ⅱ级　□ Ⅲ级　□Ⅳ级</td></tr>
<tr><td>业务影响</td><td colspan="4">□ Ⅰ级　□ Ⅱ级　□ Ⅲ级　□Ⅳ级</td></tr>
<tr><td>资产损失</td><td colspan="4">□ Ⅰ级　□ Ⅱ级　□ Ⅲ级　□Ⅳ级</td></tr>
<tr><td colspan="2">综合定级</td><td colspan="4">□ Ⅰ级　□ Ⅱ级　□ Ⅲ级　□Ⅳ级</td></tr>
<tr><td>处理过程与结果</td><td colspan="6"></td></tr>
<tr><td>建议</td><td colspan="6"></td></tr>
<tr><td rowspan="2">报告时间</td><td colspan="2">原事件上报时间</td><td colspan="4">年　月　日　时</td></tr>
<tr><td colspan="2">处理结果报告时间</td><td colspan="4">年　月　日　时</td></tr>
<tr><td>单位审查意见</td><td colspan="6">（盖章）
年　月　日</td></tr>
</table>

表 B.2（续）

以下由负责审查的主管部门填写			
备案号	No.		
备案时间	年　月　日	备案经手人	
主管部门 审查意见	（盖章） 年　月　日		
备注			

【填表说明】

1. 用户在选择处请在内划“√”；
2. 本表中位置不够填写的地方，可另附页说明。

参 考 文 献

[1] GB/T 5271.8—2001 信息技术 词汇 第8部分:安全
[2] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[3] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[4] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[5] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
[6] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求
[7] GB/T 20274.1—2006 信息安全技术 信息系统安全保障评估框架 第1部分:简介和一般模型
[8] GB/T 20275—2006 信息安全技术 入侵检测系统技术要求和测试评价方法
[9] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[10] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[11] GB/T 25070—2010 信息安全技术 信息系统等级保护安全设计技术要求
[12] BMB 17—2006 涉及国家秘密的计算机信息系统分级保护技术要求
[13] GA/T 671—2006 信息安全技术 终端计算机系统安全等级技术要求
[14] YC/Z 204—2006 烟草行业信息化标准体系
[15] 国家突发公共事件总体应急预案.国务院发布.
[16] 烟草系统特大、重大安全事故行政责任追究的规定.国烟法[2001]278号.
[17] 烟草行业信息系统技术管理规定(试行).国烟法[2001]383号.
[18] 烟草行业网络信息安全事件信息报告制度.国烟办[2009]343号.
[19] 信安秘字[2009]059号.信息系统等级保护安全设计技术要求.