ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20269—2006

信息安全技术　信息系统安全管理要求

Information security technology—
Information system security management requirements

2006-05-31 发布　　2006-12-01 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

本标准的附录A、附录B是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京思源新创信息安全资讯有限公司，江南计算技术研究所技术服务中心。

本标准主要起草人：陈冠直、王志强、吉增瑞、景乾元、宋健平。

引　言

信息安全等级保护从与信息系统安全相关的物理层面、网络层面、系统层面、应用层面和管理层面对信息和信息系统实施分等级安全保护。管理层面贯穿于其他层面之中，是其他层面实施分等级安全保护的保证。本标准对信息和信息系统的安全保护提出了分等级安全管理的要求，阐述了安全管理要素及其强度，并将管理要求落实到信息安全等级保护所规定的五个等级上，有利于对安全管理的实施、评估和检查。GB 17859—1999 中安全保护等级的划分是根据对安全技术和安全风险控制的关系确定的，公通字[2004]66 号文件中安全等级的划分是根据信息和信息系统受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成损害的程度确定的。两者的共同点是：安全等级越高，发生的安全技术费用和管理成本越高，从而预期能够抵御的安全威胁越大，建立起的安全信心越强，使用信息系统的风险越小。

本标准以安全管理要素作为描述安全管理要求的基本组件。安全管理要素是指，为实现信息系统安全等级保护所规定的安全要求，从管理角度应采取的主要控制方法和措施。根据 GB 17859—1999 对安全保护等级的划分，不同的安全保护等级会有不同的安全管理要求，可以体现在管理要素的增加和管理强度的增强两方面。对于每个管理要素，根据特定情况分别列出不同的管理强度，最多分为 5 级，最少可不分级。在具体描述中，除特别声明之外，一般高级别管理强度的描述都是在对低级别描述基础之上进行的。

信息系统是指由计算机及其相关和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行存储、传输、处理的系统或者网络；信息是指在信息系统中存储、传输、处理的数字化信息。本标准涉及信息系统的管理者包括国家机关、事业单位、厂矿企业、公司、集团等各种类型和不同规模的组织机构，以下统称为“组织机构”。

信息系统在技术上采取何种安全机制应根据相关技术标准确定，本标准仅提出保证这些安全机制实施的管理要求。与技术密切的管理是技术实现的组成部分，如果信息系统根据具体业务及其安全需求未采用该技术，则不需要相应的安全管理要求。对与管理描述难以分开的技术要求会出现在管理要求中，具体执行需要参照相关技术标准。对于涉及国家秘密的信息和信息系统的保密管理，应按照国家有关保密的管理规定和相关标准执行。

本标准中有关信息系统安全管理要素及其强度与信息系统安全管理分等级要求的对应关系的说明参见附录 A。为了帮助读者从安全管理概念角度理解和运用这些信息系统的安全管理要求，附录 B 给出了信息系统安全管理概念说明。

信息安全技术　信息系统安全管理要求

1　范围

本标准依据 GB 17859—1999 的五个安全保护等级的划分，规定了信息系统安全所需要的各个安全等级的管理要求。

本标准适用于按等级化要求进行的信息系统安全的管理。

2　规范性引用文件

下列文件中的条款通过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可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999　计算机信息系统安全保护等级划分准则

GB/T 20271—2006　信息安全技术　信息系统通用安全技术要求

3　术语和定义

GB 17859—1999 确立的以及下列术语和定义适用于本标准。

3.1

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。

3.2

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。

3.3

访问控制　access control

按确定的规则，对实体之间的访问活动进行控制的安全机制，能防止对资源的未授权使用。

3.4

安全审计　security audit

按确定规则的要求，对与安全相关的事件进行审计，以日志方式记录必要信息，并作出相应处理的安全机制。

3.5

鉴别信息　authentication information

用以确认身份真实性的信息。

3.6

敏感性　sensitivity

表征资源价值或重要性的特性，也可能包含这一资源的脆弱性。

3.7

风险评估　risk assessment

通过对信息系统的资产价值/重要性、信息系统所受到的威胁以及信息系统的脆弱性进行综合分