ICS 35.040
L 80

中华人民共和国国家标准

GB/T 19715.2—2005/ISO/IEC TR13335-2:1997

信息技术　信息技术安全管理指南 第2部分:管理和规划信息技术安全

Information technology—Guidelines for the management of IT security—Part 2:Managing and planning IT security

(ISO/IEC TR 13335-2:1997,IDT)

2005-04-19 发布　　2005-10-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　结构 …… 1
5　目的 …… 1
6　背景 …… 1
7　IT 安全管理 …… 2
8　总体 IT 安全策略 …… 3
9　IT 安全的组织方面 …… 5
10　总体风险分析战略选项 …… 7
11　IT 安全建议 …… 8
12　IT 系统安全策略 …… 9
13　IT 安全计划 …… 10
14　实施防护措施 …… 10
15　安全意识 …… 11
16　后续活动 …… 11
17　小结 …… 13

前　言

GB/T 19715《信息技术　信息技术安全管理指南》分为五个部分：

——第1部分：信息技术安全概念和模型；

——第2部分：管理和规划信息技术安全；

——第3部分：信息技术安全管理技术；

——第4部分：防护措施的选择；

——第5部分：外部连接的防护措施。

本部分等同采用国际标准ISO/IEC TR 13335-2:1997《信息技术　信息技术安全管理指南　第2部分：管理和规划信息技术安全》。

本部分中的指南提出IT安全管理的一些基本专题以及这些专题之间的关系。这些指南对标识和管理IT安全各个方面是有用的。

本部分由中华人民共和国信息产业部提出。

本部分由全国信息安全标准化技术委员会归口。

本部分由中国电子技术标准化研究所(CESI)、中国电子科技集团第十五研究所、中国电子科技集团第三十研究所、上海三零卫士信息安全有限公司负责起草。

本部分主要起草人：安金海、林中、林望重、魏忠、罗锋盈、陈星。

引　言

GB/T 19715 的目的是提供关于 IT 安全管理方面的指南，而不是解决方案。那些在组织内负责 IT 安全的个人应该可以采用本标准中的资料来满足他们特定的需求。本标准的主要目标是：

a) 定义和描述与 IT 安全管理相关的概念；

b) 标识 IT 安全管理和一般的 IT 管理之间的关系；

c) 提出了几个可用来解释 IT 安全的模型；

d) 提供了关于 IT 安全管理的一般的指南。

本标准由多个部分组成。第 1 部分提供了描述 IT 安全管理用的基本概念和模型的概述。本部分适用于负责 IT 安全的管理者及那些负责组织的总体安全大纲的管理者。

本部分描述了管理和规划方面。它和负责组织的 IT 系统的管理者相关。他们可以是：

a) 负责监督 IT 系统的设计、实施、测试、采购或运行的 IT 管理者；

b) 负责制定 IT 系统的实际使用活动的管理者；

c) 当然还有负责 IT 安全的管理者。

第 3 部分描述了在一个项目的生存周期(比如规划、设计、实施、测试、采办或运行)所涉及的管理活动中适于使用的安全技术。

第 4 部分提供了选择防护措施的指南，以及通过基线模型和控制的使用如何受到支持。它也描述了它如何补充了第 3 部分中描述的安全技术，如何使用附加的评估方法来选择防护措施。

第 5 部分为组织提供了将它的 IT 系统连接到外部网络的指南。该指南包含了提供连接安全的防护措施的选择、使用，那些连接所支持的服务，以及进行连接的 IT 系统的附加防护措施。

信息技术　信息技术安全管理指南
第2部分:管理和规划信息技术安全

1　范围

GB/T 19715的本部分提出IT安全管理的一些基本专题以及这些专题之间的关系。这些部分对标识和管理IT安全各个方面是有用的。

熟悉第1部分所介绍的概念和模型对全面理解本部分是重要的。

2　规范性引用文件

下列文件中的条款通过GB/T 19715的本部分的引用而成为本部分的条款。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部分,然而,鼓励根据本部分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部分。

GB/T 19715.1—2005　信息技术　信息技术安全管理指南　第1部分:信息技术安全概念和模型(ISO/IEC TR 13335-1:1996,IDT)

3　术语和定义

GB/T 19715.1—2005确立的术语和定义适用于本部分,使用其下列术语:可核查性、资产、真实性、可用性、基线控制、保密性、数据完整性、影响、完整性、IT安全、IT安全策略、可靠性、残留风险、风险、风险分析、风险管理、防护措施、系统完整性、威胁、脆弱性。

4　结构

本部分有17章。第5章和第6章提供有关本文件目的和背景方面的信息。第7章提供成功的IT安全管理中所涉及的各种活动的概述。第8章到第16章详述这些活动。第17章提供小结。

5　目的

本部分的目的是要提出与IT安全管理和规划有关的各种活动,以及组织中有关的角色和职责。这一般与负责IT系统采购、设计、实现或运行的IT管理人员有关。除了IT安全管理人员外,还与负责使IT系统具体使用活动的管理人员有关。总之,本部分对与组织IT系统有关的负管理责任的任何人是有用的。

6　背景

为进行业务活动,政府和商业组织极其依赖信息的使用。信息和服务的保密性、完整性、可用性、可核查性、真实性和可靠性的损失会给组织带来负面影响。因此,在组织中对保护信息和管理信息技术(IT)的安全有着重要的需求。在现今环境中,保护信息的这一要求尤为重要,因为许多组织通过IT系统的网络进行内部和外部的连接。

IT安全管理是用来实现和维护保密性、完整性、可用性、可核查性、真实性和可靠性相应等级过程的。IT安全管理功能包括:

a)　确定组织IT安全目标、战略和策略;