ICS 35.040
L 80

中华人民共和国国家标准

GB/T 19715.1—2005/ISO/IEC TR 13335-1:1996

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

Information technology—Guidelines for the management of IT security—Part 1:Concepts and models of IT security

(ISO/IEC TR 13335-1:1996,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

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 13335-1:1996《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》。

本部分提出基本的管理概念和模型，将这些概念和模型引入信息技术安全管理是必要的。

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。

GB/T 19715 由多个部分组成。本部分为第 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。

第 2 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。

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1部分:信息技术安全概念和模型

1　范围

GB/T 19715包含IT安全管理的指南。本部分提出了基本的管理概念和模型,将这些概念和模型引入IT安全管理是必要的。在指南的其余部分还将进一步讨论和开发这些概念和模型以提供更详细的指南。为有助于标识和管理IT安全的各个方面可以同时使用本标准的各部分。本部分对全面理解本标准的后续各部分是必需的。

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 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分:安全体系结构(idt ISO 7498-2:1989)

3　术语和定义

下列术语和定义适用于GB/T 19715的各个部分。

3.1

可核查性　accountability

确保可将一个实体的行动唯一地追踪到此实体的特性[GB/T 9387.2—1995]。

3.2

资产　asset

对组织具有价值的任何东西。

3.3

真实性　authenticity

确保主体或资源的身份是所声称身份的特性。真实性适用于诸如用户、过程、系统和信息这样的实体。

3.4

可用性　availability

已授权实体一旦需要就可访问和使用的特性[GB/T 9387.2—1995]。

3.5

基线控制　baseline controls

为一个系统或组织建立的防护措施的最小集合。

3.6

保密性　confidentiality

使信息不泄露给未授权的个人、实体、过程或不使信息为其利用的特性。