ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25068.1—2012/ISO/IEC 18028-1:2006

信息技术　安全技术　IT网络安全 第1部分:网络安全管理

Information technology—Security techniques—IT network security—Part 1:Network security management

(ISO/IEC 18028-1:2006,IDT)

2012-06-29 发布　　2012-10-01 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

中 华 人 民 共 和 国
国 家 标 准
信息技术 安全技术 IT 网络安全
第 1 部分:网络安全管理
GB/T 25068.1—2012/ISO/IEC 18028-1:2006
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:010-68522006
2012 年 10 月第一版
*
书号:155066·1-45562

目　　次

前　言

GB/T 25068《信息技术　安全技术　IT 网络安全》分为以下 5 个部分：

——第 1 部分：网络安全管理；

——第 2 部分：网络安全体系结构；

——第 3 部分：使用安全网关的网间通信安全保护；

——第 4 部分：远程接入的安全保护；

——第 5 部分：使用虚拟专用网的跨网通信安全保护。

本部分为 GB/T 25068 的第 1 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用翻译法等同采用国际标准 ISO/IEC 18028-1:2006《信息技术　安全技术　IT 网络安全　第 1 部分：网络安全管理》。

本部分作了以下纠正：在第 4 章的缩略语中纠正一个缩略语的英文原文。纠正的缩略语的英文原文在所在页的边空白处用单竖线“|”标出。13.3.1 中原文有误，已纠正，在页边用单竖线“|”指示。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/Z 20985—2007　信息技术　安全技术　信息安全事件管理指南(ISO/IEC TR 18044:2004,MOD)。

——GB/T 28454—2012　信息技术　安全技术　入侵检测系统的选择、部署和操作(ISO/IEC 18043:2006,MOD)

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。

本部分由全国信息安全标准化技术委员会(TC 260)提出并归口。

本部分起草单位：黑龙江省电子信息产品监督检验院、中国电子技术标准化研究所。

本部分主要起草人：王希忠、姜波、黄俊强、马遥、方舟、王大萌、树彬、张清江、宋超臣、段志鸣、上官晓丽、许玉娜、王运福、吴梅艳。

引　言

通信和信息技术业界一直在寻找经济有效的全面安全解决方案。安全的网络应受到保护，免遭恶意和无意的攻击，并且应满足业务对信息和服务的保密性、完整性、可用性、抗抵赖、可核查性、真实性和可靠性的要求。保护网络安全对于适当维护计费或使用信息的准确性也是必要的。产品的安全保护能力对于全网的安全（包括应用和服务）是至关重要的。然而，当更多的产品被组合起来以提供整体解决方案时，互操作性的优劣将决定这种解决方案的成功与否。安全不仅是对每种产品或服务的关注，还必须以促进全面的端到端安全解决方案中各种安全能力交合的方式来开发。因此，GB/T 25068 的目的是为 IT 网络的管理、操作和使用及其互连等安全方面提供详细指南。组织中负责一般 IT 安全和特定 IT 网络安全的人员应能够调整 GB/T 25068 中的材料以满足他们的特定要求。GB/T 25068 的主要目标如下：

——GB/T 25068.1 定义和描述网络安全的相关概念，并提供网络安全管理指南——包括考虑如何识别和分析与通信相关的因素以确立网络安全要求，还介绍可能的控制领域和特定的技术领域（相关内容在 GB/T 25068 的后续部分中涉及）；

——GB/T 25068.2 定义一个标准的安全体系结构，它描述一个支持规划、设计和实施网络安全的一致框架；

——GB/T 25068.3 定义使用安全网关保护网络间信息流安全的技术；

——GB/T 25068.4 定义保护远程接入安全的技术；

——GB/T 25068.5 定义对使用虚拟专用网（VPN）建立的网络间连接进行安全保护的技术。

GB/T 25068.1 与涉及拥有、操作或使用网络的所有人员相关。除了对信息安全（IS）和/或网络安全及网络操作负有特定责任的、或对组织的全面安全规划和安全策略开发负有责任的管理者和管理员外，还包括高级管理者和其他非技术性管理者或用户。

GB/T 25068.2 与涉及规划、设计和实施网络安全体系结构方面的所有人员（例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管）相关。

GB/T 25068.3 与涉及详细规划、设计和实施安全网关的所有人员（例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管）相关。

GB/T 25068.4 与涉及详细规划、设计和实施远程接入安全的所有人员（例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管）相关。

GB/T 25068.5 与涉及详细规划、设计和实施 VPN 安全的所有人员（例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管）相关。

信息技术　安全技术　IT网络安全
第1部分:网络安全管理

1　范围

GB/T 25068的本部分规定了网络和通信安全方面的指导,包括信息系统网络自身的互连以及将远程用户连接到网络。

本部分适用于那些负责信息安全管理,尤其是网络安全管理的相关人员。本部分支持识别和分析与通信相关的因素,这些因素宜在建立网络安全要求时考虑到;针对与通信网络连接相关的安全,介绍如何识别适当的控制域;综述可能的控制域,包括在GB/T 25068.2至GB/T 25068.5中详细论述的那些技术设计和实施主题。

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/T 22081—2008　信息技术　安全技术　信息安全管理实用规则(ISO/IEC 27002:2005,IDT)

GB/T 25068.2—2012　信息技术　安全技术　IT网络安全　第2部分:网络安全体系结构(ISO/IEC 18028-2:2005,IDT)

GB/T 25068.3—2010　信息技术　安全技术　IT网络安全　第3部分:使用安全网关的网间通信安全保护(ISO/IEC 18028-3:2005,IDT)

GB/T 25068.4—2010　信息技术　安全技术　IT网络安全　第4部分:远程接入的安全保护(ISO/IEC 18028-4:2005,IDT)

GB/T 25068.5—2010　信息技术　安全技术　IT网络安全　第5部分:使用虚拟专用网的跨网通信安全保护(ISO/IEC 18028-5:2006,IDT)

ISO/IEC 18043:2006　信息技术　安全技术　入侵检测系统的选择、部署和操作(Information technology—Security techniques—Selection, deployment and operations of intrusion detection systems)

ISO/IEC TR 18044:2004　信息技术　安全技术　信息安全事件管理指南(Information technology—Security techniques—Information security incident management)

ISO/IEC 13335-1:2004　信息技术　安全技术　信息和通信技术安全管理　第1部分:信息和通信技术安全管理概念和模型(Information technology—Security techniques—Management of information and communications technology security—Part 1:Concepts and models for information and communications technology security management)

3　术语和定义

3.1　其他标准中的术语和定义

GB/T 9387(所有部分)和GB/T 22081中界定的术语和定义适用于本文件。