ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25068.2—2012/ISO/IEC 18028-2:2006

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

Information technology—Security techniques—IT network security—Part 2:Network security architecture

(ISO/IEC 18028-2:2006,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

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 2 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 18028-2:2006《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》。

根据国情和 GB/T 1.1 的规定，做了如下一些编辑性修改：

——原文 CCITT X.800 中的内容已在本部分引用的国家标准 GB/T 9387.2—1995 中体现，故本部分不再引用 X.800。

——在原文正文里使用的缩略语没有全部反映在第 4 章中，本部分在其中做了增补，增加的缩略语在其页边切口用单竖线“|”指示。

——为避免干扰章节编号，第 5 章中几个问题的数字编号改为字母编号。

——由于我国尚未有隐私和数据保护的相关法律法规，故在 6.8 中删掉“依据国家隐私和数据保护的法律法规”。

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：黄俊强、王希忠、方舟、马遥、王大萌、张清江、宋超臣、段志鸣、树彬、上官晓丽、许玉娜、王运福。

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，互操作性将决定这种解决方案的成功与否。安全不一定只是对每种产品或服务的单线关注，而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织的方式来开发。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2部分:网络安全体系结构

1　范围

GB/T 25068的本部分规定了用于提供端到端网络安全的网络安全体系结构。

本部分适用于体系结构能应用于关注端到端安全且独立于网络下层技术的各种类型的网络。其目的是作为开发详细的端到端网络安全建议的基础。

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 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(ISO 7498-2:1989,IDT)。

3　术语和定义

GB/T 9387.2—1995中界定的下列术语和定义适用于本文件。

3.1

访问控制　access control

防止未授权使用资源,包括防止以未授权方式使用某一资源。

3.2

数据原发鉴别　data origin authentication

确认接收到的数据的来源是所声称的。

3.3

对等实体鉴别　peer-entity authentication

确认某一关联中的对等实体是所声称的实体。

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。

3.5

保密性　confidentiality

使信息不泄漏给未授权的个人、实体或过程或不使信息为其利用的特性。

3.6

数据完整性　data integrity

数据未经未授权方式修改或破坏的特性。