ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25068.2—2020/ISO/IEC 27033-2:2012
代替 GB/T 25068.2—2012

信息技术　安全技术　网络安全 第2部分:网络安全设计和实现指南

Information technology—Security techniques—Network security—Part 2: Guidelines for the design and implementation of network security

(ISO/IEC 27033-2:2012,IDT)

2020-11-19 发布　　2021-06-01 实施

国家市场监督管理总局
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　网络安全》目前分为以下5部分：

——第1部分：综述和概念；

——第2部分：网络安全设计和实现指南；

——第3部分：参考网络场景——风险、设计技术和控制要素；

——第4部分：使用安全网关的网间通信安全保护；

——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。

本部分代替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》，与GB/T 25068.2—2012相比，主要技术变化如下：

——删除了“网络安全参考体系结构”“安全维”“安全层”“安全面”“安全威胁”“对安全维应用于安全层所实现目标的描述”等内容，增加了“文档结构”“网络安全设计准备”“网络安全设计”“网络安全实现”等内容（见第5章～第8章，2012年版的第5章～第10章）；

——修改了第1章范围的内容（见第1章，2012年版的第1章）；

——删除了规范性引用文件GB/T 9387.2-1995的引用，增加了ISO/IEC 27000:2009、ISO/IEC 27001:2005、ISO/IEC 27002:2005、ISO/IEC 27005:2011、ISO/IEC 7498（所有部分）、ISO/IEC 27033-1的引用（见第2章，2012年版的第2章）；

——删除了第3章的术语和定义，修改了引导语（见第3章，2012年版的第3章）；

——删除了“ASP”“ATM”“DHCP”“DNS”“DS-3”“Ipsec”“MD5”“Megaco/H.248”“MPLS”“OAM&P”“OSI”“POP”“PSTN”“PVC”“QoS”“SHA-1”“SIP”“SNMP”“SONET”“SS7”“SSL”“VLAN”等缩略语，增加了“IPS”“POC”“RADIUS”“SMS”“TACACS”“TFTP”等缩略语（见第4章，2012年版的第4章）。

本部分使用翻译法等同采用ISO/IEC 27033-2:2012《信息技术　安全技术　网络安全　第2部分：网络安全设计和实现指南》。

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/T 9387（所有部分）　信息技术　开放系统互连　基本参考模型[ISO/IEC 7498（所有部分），IDT]；

——GB/T 22080—2016　信息技术　安全技术　信息安全管理体系　要求（ISO/IEC 27001:2013，IDT）；

——GB/T 22081—2016　信息技术　安全技术　信息安全控制实践指南（ISO/IEC 27002:2013，IDT）；

——GB/T 25068.1—2020　信息技术　安全技术　网络安全　第1部分：综述和概念（ISO/IEC 27033-1:2015，IDT）；

——GB/T 29246—2017　信息技术　安全技术　信息安全管理体系 概述和词汇（ISO/IEC 27000:2016，IDT）；

——GB/T 31722—2015　信息技术　安全技术　信息安全风险管理（ISO/IEC 27005:2008，IDT）。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位:黑龙江省网络空间研究中心、中国电子技术标准化研究所、北京安天网络安全技术有限公司、杭州安恒信息技术有限公司、哈尔滨理工大学、西安西电捷通无线网络通信股份有限公司。

本部分主要起草人:曲家兴、方舟、谷俊涛、张宏国、李锐、宋雪、马遥、王大萌、吴琼、树彬、刘佳、姜国春、冯亚娜、张弘、司丹、张驰、于海宁。

本部分所代替标准的历次版本发布情况为:

——GB/T 25068.2—2012。

信息技术　安全技术　网络安全
第2部分:网络安全设计和实现指南

1　范围

GB/T 25068的本部分为组织给出了计划、设计、实施和记录网络安全的指南。

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。

ISO/IEC 7498(所有部分)　信息技术　开放系统互连　基本参考模型(Information technology—Open systems interconnection—Basic reference model)

ISO/IEC 27000:2009　信息技术　安全技术　信息安全管理体系　概述和词汇(Information technology—Security techniques—Information security management systems—Overview and vocabulary)

ISO/IEC 27001:2005　信息技术　安全技术　信息安全管理体系　要求(Information technology—Security techniques—Information security management systems—Requirements)

ISO/IEC 27002:2005　信息技术　安全技术　信息安全管理实用规则(Information technology—Security techniques—Code of practice for information security management)

ISO/IEC 27005:2011　信息技术　安全技术　信息安全风险管理(Information technology—Security techniques—Information security risk management)

ISO/IEC 27033-1　信息技术　安全技术　网络安全　第1部分:综述和概念(Information technology—Security techniques—Network security—Part 1:Overview and concepts)

3　术语和定义

ISO/IEC 7498(所有部分)、ISO/IEC 27000:2009、ISO/IEC 27001:2005、ISO/IEC 27002:2005、ISO/IEC 27005:2011和ISO/IEC 27033-1界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

IPS:入侵防御系统(Intrusion Prevention System)

POC:概念证明(Proof of Concept)

RADIUS:远程认证拨号用户服务(Remote Authentication Dial-In User Service)

RAS:远程访问服务(Remote Access Service)

SMS:简单消息服务(Simple Message Service)

SMTP:简单邮件传输协议(Simple Mail Transfer Protocol)

TACACS:终端访问控制器访问控制系统(Terminal Access Controller Access-Control System)