ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 25068.3—2022
代替 GB/T 25068.4—2010

信息技术　安全技术　网络安全 第3部分：面向网络接入场景的威胁、设计技术和控制

Information technology—Security techniques—Network security—Part 3：Threats，design techniques and control for network access scenarios

（ISO/IEC 27033-3：2010，Information technology—Security techniques—Network security—Part 3：Reference networking scenarios—Threats，design techniques and control issues，MOD）

2022-10-12 发布　　2023-05-01 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

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 25068《信息技术 安全技术 网络安全》的第3部分。GB/T 25068已发布了以下部分：

——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：面向网络接入场景的威胁、设计技术和控制；

——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。

本文件代替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》。与GB/T 25068.4—2010相比，除结构调整和编辑性改动外，主要技术变化如下：

——本文件主要内容由远程接入的安全保护改为面向网络接入场景的威胁、设计技术和控制；

——本文件对原系列标准中的每个技术应用场景进行了重新归纳和修改；

——删除了“接入点”“高级加密标准”“回叫”等术语和定义，增加了“恶意软件”“不透明性”“外包”等术语和定义（见第3章，2010年版的第3章）；

——增加了“员工的互联网访问服务”“企业对企业的服务”“企业对客户的服务”“增强协作服务”“网络分段”“为居家办公和小型商务办公场所提供网络支持”等内容，删除了“远程访问连接类型”“远程访问连接技术”“选择和配置指南”等内容（见第7章～第15章，2010年版的第6章～第8章）；

——增加了“威胁目录”“互联网使用策略示例”，删除了“远程接入安全策略示例”“RADIUS实施和部署的最佳实践”“FTP的两种模式”“安全邮件服务核查表”“安全Web服务核查表”“无线局域网安全核查表”（见附录A、附录B，2010年版的附录A～附录F）。

本文件修改采用ISO/IEC 27033-3：2010《信息安全　安全技术　网络安全　第3部分：参考网络场景—威胁、设计技术和控制》。

本文件与ISO/IEC 27033-3：2010相比做了下述结构调整：

——将附录A调整为附录B，附录B调整为附录A。

本文件与ISO/IEC 27033-3：2010的技术差异及其原因如下：

——用规范性引用的GB/T 29246代替ISO/IEC 27000（见第3章、第6章），GB/T 25068.1代替ISO/IEC 27033-1（见第3章），以适应我国的技术条件；

——将面向联邦国家或欧盟等政府组织的网络分段指导改为适合我国的跨国组织的网络分段指导，并以“注”的形式出现（见11.1）。

本文件做了下列编辑性改动：

——将一些适用于国际标准的表述改为适用于我国标准的表述；

——增加了表1中的脚注；

——将国际标准附录A中面向博客的使用要求扩展为面向所有社交平台的使用要求；

——将国际标准附录A中A.4.3中的悬置段调整为附录B中带序号的B.4.3.1等内容；

——删除了国际标准附录A中的定义A.6；

——增加了“参考文献”。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位:黑龙江省网络空间研究中心、中国电子技术标准化研究院、安天科技集团股份有限公司、黑龙江安信与诚科技开发有限公司、上海工业控制安全创新科技有限公司、哈尔滨理工大学、哈尔滨工业大学。

本文件主要起草人:曲家兴、方舟、于海宁、谷俊涛、肖鸿江、李琳琳、宋雪、李锐、杨霄璇、白瑞、马遥、王大萌、呼大永、树彬、吴琼、上官晓丽、蔡一鸣、杜宇芳、赵超、吴佳兴、曹威、鲁子元、马超、孟庆川、单建中、韩建雍、刘明鸽、黄海、方伟、童松华、刘颖、孙腾、倪华。

本文件及其所代替文件的历次版本发布情况为:

——2010 年首次发布为 GB/T 25068.4—2010;

——本次为第一次修订,调整为 GB/T 25068.3—2022。

引　言

GB/T 25068 的目的是为信息系统网络的管理、运行、使用及互联互通提供安全方面的详细指导，方便组织内负责信息安全特别是网络安全的人员采纳本文件以满足其特定需求。拟由六个部分构成。

——第 1 部分：综述和概念。目的是提出网络安全相关的概念并提供管理指导。

——第 2 部分：网络安全设计和实现指南。目的是为组织如何规划、设计、实现高质量的网络安全体系，确保网络安全适合相应的业务环境提供指导。

——第 3 部分：面向网络接入场景的威胁、设计技术和控制。目的是列举与典型的网络接入场景相关的具体风险、设计技术和控制，适用于所有参与网络安全架构方面规划、设计和实施的人员。

——第 4 部分：使用安全网关的网间通信安全保护。目的是确保使用安全网关的网间通信安全。

——第 5 部分：使用虚拟专用网的跨网通信安全保护。目的是定义使用虚拟专用网络建立安全连接的具体风险、设计技术和控制要素。

——第 6 部分：无线网络访问安全。目的是为选择、实施和监测使用无线网络提供安全通信所必需的技术控制提供指南，并用于第 2 部分中涉及使用无线网络的技术安全架构或设计选项的审查与选择。

GB/T 25068 是在 GB/T 22081《信息技术　安全技术　信息安全控制实践指南》的基础上，进一步对网络安全控制提供了详细的实施指导。GB/T 25068 仅强调业务类型等因素影响网络安全的重要性而不做具体说明。

本文件凡涉及采用密码技术解决保密性、完整性、真实性、抗抵赖性需求的，遵循密码相关国家标准和行业标准。

信息技术　安全技术　网络安全 第3部分:面向网络接入场景的威胁、设计技术和控制

1　范围

本文件描述了与网络接入场景相关的威胁、设计技术和控制问题,为每一个网络接入场景提供了能够降低相关风险的安全威胁、安全设计技术以及控制三个要素的详细指南。

本文件适用于按照GB/T 25068.2来评审技术性安全体系的结构和设计,以及选择和记录首选技术安全架构、设计和相关控制的选项。被评审的网络环境的特征决定了特定信息的选择(包括从GB/T 25068.4、GB/T 25068.5及ISO/IEC 27033-6中选择的信息),即特定信息的选择与特定网络接入场景和"技术"主题有关。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 29246　信息技术　安全技术　信息安全管理体系　概述和词汇(GB/T 29246—2017,ISO/IEC 27000:2016,IDT)

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

3　术语和定义

GB/T 29246、GB/T 25068.1界定的以及下列术语和定义适用于本文件。

3.1

恶意软件　malware

带有恶意设计的软件类别,包含可能直接或间接对用户或用户的计算机系统造成潜在伤害的特性或功能。

[来源:ISO/IEC 27032:2012,4.35]

3.2

不透明性　opacity

对可能通过监测网络活动(例如在互联网上的VoIP呼叫中获得端点的地址)获得的信息给予保护。

注:不透明性同时还保护获得信息的相关行为。