ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25068.1—2020/ISO/IEC 27033-1:2015
代替 GB/T 25068.1—2012

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

(ISO/IEC 27033-1:2015,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1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 25068.1—2012《信息技术　安全技术　IT网络安全　第1部分：网络安全管理》。与GB/T 25068.1—2012相比，主要技术变化如下：

——增加了“支持控制”“参考网络场景—风险、设计技术和控制要素”“开发和测试安全解决方案”等内容，删除了“目标”“公共基础设施中基于密码的服务”等内容（见第8章、第10章、第12章，2012年版的第2章、第13章）；

——删除了对GB/T 22081—2008、GB/T 25068.2—2012、GB/T 25068.3—2010的注日期引用，增加了对ISO/IEC 27000、ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005的不注日期引用（见第2章，2012年版的第2章）；

——删除了“安全维”“滥发”等术语和定义，增加了“架构”“信息安全策略”等术语和定义（见第3章，2012年版的第3章）；

——删除了“Telnet”“TETRA”等缩略语，增加了“BPL”“CA”“DPNSS”等缩略语（见第4章，2012年版的第4章）；

——删除了网络连接类型、信任关系的识别、信任关系参考、潜在脆弱性类型，增加了网络安全风险区域的概念模型、网络安全风险评估和管理过程（见第5章～第8章，2012年版第7章、第10章～第12章）；

——增加了本部分中安全控制部分同ISO/IEC 27001、ISO/IEC 27002中相关条款交叉引用及SecOPs文档示例模板（见附录A、附录B）。

本部分使用翻译法等同采用ISO/IEC 27033-1:2015《信息安全 安全技术　网络安全　第1部分：综述和概念》。

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）]；

——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 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）。

本部分做了下列编辑性修改：

——在第2章增加了正文中规范引用的国际文件ISO/IEC 27000。

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院、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：方舟、曲家兴、马超、谷俊涛、树彬、刘佳、李锐、宋雪、马遥、王大萌、吴琼、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 25068.1—2012。

引　言

当前，商业和政府组织大多数都通过网络连接他们的信息系统（如图 1 所示），其中，网络连接类型可能包括如下一个或多个：

——组织内部的网络；

——不同组织间的网络；

——组织和公众之间的网络。

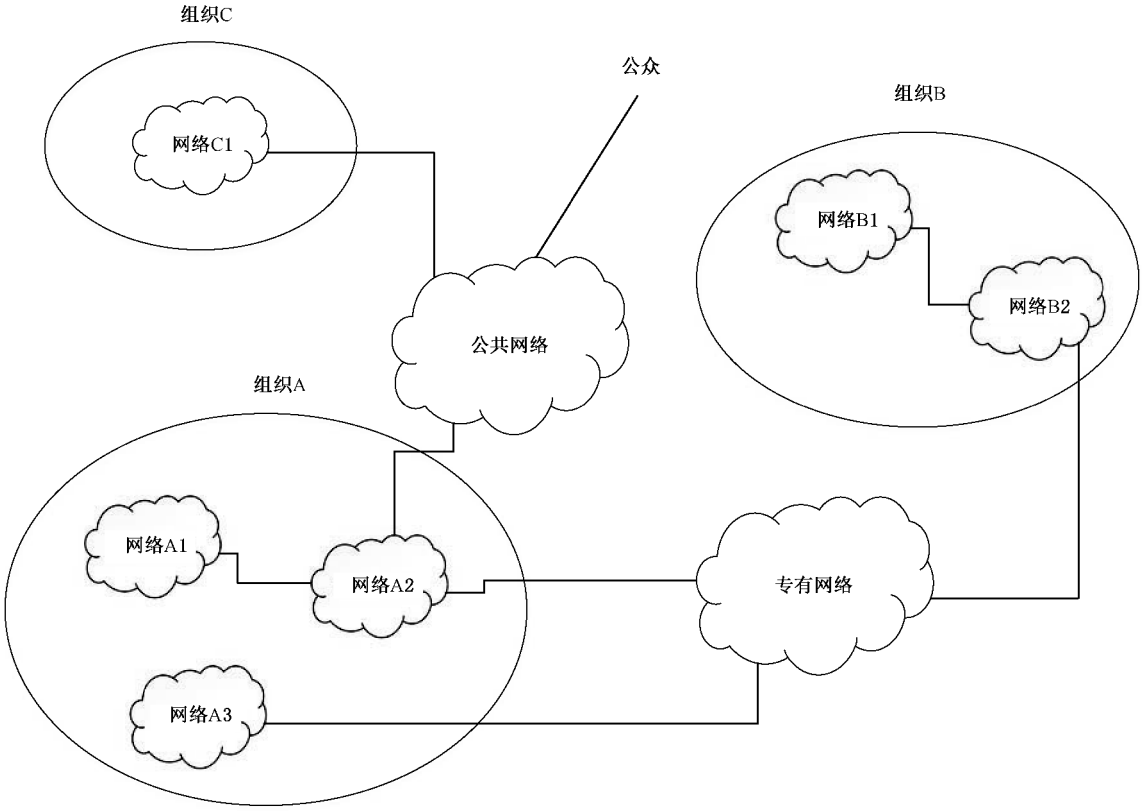

图 1　典型的网络类型及连接方式

此外，快速发展的网络技术（特别是通过互联网发展起来网络技术）提供了重要商业机会，越来越多的组织机构开展全球性的电子商务以提供在线公共服务。这些商业机会不仅实现了将互联网作为简单的连接媒介以提供低成本的数据通信，也实现了由互联网服务提供商（ISP）提供更复杂的服务。这也就意味着，通过在电路的每一端使用相对低成本的本地连接，可完整实现在线电子交易和服务交付系统，例如采用基于 Web 的应用及服务技术。此外，新的技术（包括数据、语音和视频的集成）为远程工作提供了可能（也称为“远程工作”或“远程办公”），使员工能够在一段时间内离开他们的工作地点，还能通过远程设备访问组织网络、社区网络，以及相关业务支持信息和服务。

这种环境有利于获得重大商业利益，但又存在新的安全风险。随着组织越来越依赖于信息和相关网络，那么信息保密性、完整性及可用性的缺失将会对开展业务造成极大负面影响。因此，有必要适当保护网络、信息系统和信息的安全。换句话说，实施和维护充分的网络安全对任何组织业务稳定运行来说都是至关重要的。

在这种情况下，电信和信息技术产业正在寻求成本效益均衡的安全解决方案，旨在保护网络免受恶意攻击和无意的不正当行为，满足信息和服务保密性、完整性和可用性的业务要求。适当的网络安全对于确保服务计费和使用信息的准确性是必不可少的。产品的安全能力对整体网络安全（包括应用和服务）至关重要，然而，随着更多解决方案将产品组合起来形成的一个整体，产品间是否具备互操作性将决定解决方案成功与否。安全性是每个产品或服务的关注点，它是依靠提高整体安全解决方案的安全能力进行开发。

ISO/IEC 27033[1)]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。组织内负责信息安全，特别是网络安全的人员宜能够采纳本标准以满足其特定需求。其主要目标如下：

——ISO/IEC 27033-1，定义和描述与网络安全相关的概念并提供管理指导。包括网络安全概述及相关定义，指导网络安全风险识别和分析，进而定义网络安全需求。它还介绍了如何达成优质的技术安全架构，以及与典型网络场景和网络“技术”领域相关的风险、设计和控制等方面（ISO/IEC 27033 其余部分将详细介绍）；

——ISO/IEC 27033-2，定义了组织宜如何规划、设计、实现高质量的网络安全体系，以确保网络安全适合相应的业务环境。可借助模型框架（本部分标准利用模型框架来描述一类技术安全架构、设计的结构和内部运行机制），使用一致的方法，进行网络安全规划、设计与实现。同时，本部分标准也适用于参与到网络安全规划、设计和实施网络安全架构的人员参考（例如，网络架构师、设计人员、网络管理员和网络安全主管）；

——ISO/IEC 27033-3，定义与典型的网络场景相关的具体风险、设计技术和控制要素，与所有参与网络安全架构方面规划、设计和实施的人员（例如，网络架构师、设计人员、网络管理员和网络安全主管有关）；

——ISO/IEC 27033-4，定义使用安全网关保护的网络之间信息流的具体风险、设计技术和控制要素。与所有参与安全网关的详细规划、设计和实施的人员（例如，网络架构师、设计人员、网络管理员和网络安全主管）有关；

——ISO/IEC 27033-5，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。这与所有参与 VPN 安全性详细规划、设计和实施的人员（例如，网络架构师、设计人员、网络管理员和网络安全主管）有关；

——ISO/IEC 27033-6，定义保护 IP 无线网络的具体风险、设计技术和控制要素。与参与详细规划、设计和实施无线网络安全的人员（例如，网络架构师、设计人员、网络管理员和网络安全主管）有关。

宜强调的是，ISO/IEC 27033 是在 ISO/IEC 27002 的基础上，进一步对网络安全控制提供了详细的实施指导。

宜注意的是，ISO/IEC 27033 不是法规和立法要求的参考或规范性文件。因为网络安全取决于业务类型等因素，所以仅强调这些影响的重要性而不做具体说明。

ISO/IEC 27033 凡涉及采用密码技术解决保密性、完整性、真实性、抗抵赖性需求的宜遵循密码相关国家标准和行业标准。

除非另做说明，ISO/IEC 27033 的本部分所参考的指南仅适用于当前和/或规划的“网络”或“此网络”。

1） 目前，ISO/IEC 27033 的第 1 部分～第 5 部分已转化为 GB/T 25068.1～GB/T 25068.5。

信息技术　安全技术　网络安全
第1部分:综述和概念

1　范围

GB/T 25068的本部分规定了网络安全概述和相关定义、定义和描述了与网络安全相关的概念并提供了有关网络安全的管理指导(本部分的网络安全适用于通过通信链路传送的信息安全、设备安全以及与设备、应用/服务和最终用户相关的管理活动的安全)。

本部分的使用者包括拥有、运行或使用网络的任何人,包括高级管理人员和其他非技术管理人员或用户,以及对信息安全和/或网络安全、网络操作负有特定责任的或对组织的整体安全计划和安全策略制定负责的经理和管理员。此外,还包括参与网络安全架构方面的规划、设计和实施的所有人。

本部分还包括以下内容:

——提供了识别和分析网络安全风险的指南,并基于上述分析定义网络安全需求;

——提供了支持网络技术安全架构和相关技术控制的综述,以及不仅适用于网络的技术和非技术控制;

——介绍了如何实现高质量的网络技术安全架构,以及与典型网络场景和网络"技术"领域相关的风险、设计和控制要素(在GB/T 25068的其他部分中详细论述),简述了与实施和运行网络安全控制有关的问题,以及对其实施进行持续监督和评审的相关问题。

本部分提供了GB/T 25068系列标准的概述和对其他部分的指引。

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:命名与编址(Information technology—Open systems interconnection—Basic reference model:Naming and addressing)

ISO/IEC 27000　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　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　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 controls)

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

3　术语和定义

ISO/IEC 7498(所有部分)、ISO/IEC 27000、ISO/IEC 27001、ISO/IEC 27002、ISO/IEC 27005界定的以及下列术语和定义适用于本文件。

注:以下术语及定义同样适用于GB/T 25068的其他部分。