ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32920—2016/ISO/IEC 27010:2012

信息技术　安全技术　行业间和组织间通信的信息安全管理

Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications

(ISO/IEC 27010:2012,IDT)

2016-08-29 发布　　2017-03-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准使用翻译法等同采用国际标准 ISO/IEC 27010:2012《信息技术　安全技术　行业间和组织间通信的信息安全管理》(英文版)。根据 GB/T 1.1—2009 和 GB/T 20000.2—2009 的规定,做了如下一些编辑性修改:

——在本标准的引言中,添加“标准中‘针对行业间和组织间通信没有附加的信息’,指的是 GB/T 22081—2008中对应条款没有附加的信息”;

——在本标准的第 3 章中,添加 3.2 缩略语;

——在本标准附录 B.3 中,“该方法的有效性已得到英国国家基础设施保护中心确认,并用于自动配置和分发预警信息给各类信息共享团体”放到脚注中;

——在本标准附录 C 中,“此描述是从欧洲网络和信息安全局(ENISA)发布的网络安全信息交换的良好实践指南中获得的,概念最初是由英国的国家基础设施保护中心(CPNI)制定的”放到脚注中;

——在本标准 4.2 和 7.3.3 中,分别添加参见附录 A 和参见附录 B,以符合 GB/T 1.1—2009 中提到“每个附录均应在正文或前言的相关条文中明确提及”。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东省标准化研究院、厦门市美亚柏科信息股份有限公司、中国信息安全认证中心、江苏省电子信息产品质量监督检验研究院、贵州大学、泰安市技术监督情报所。

本标准主要起草人:王曙光、王庆升、公伟、隗玉凯、栾江霞、吴鸿伟、魏军、李旭、李智、赵倩倩、黄申、吴兰、潘平、杨平。

引　言

本标准是对 GB/T 22080—2008（ISO/IEC 27001：2005，IDT）和 GB/T 22081—2008（ISO/IEC 27002:2005,IDT)在信息共享团体中使用的补充。本标准包含的指南不包括信息安全管理体系(ISMS)标准族内其他标准中给出的通用指南,并与之互为补充。

GB/T 22080—2008 和 GB/T 22081—2008 采用一种通用的方式处理组织间的信息交换。当组织希望与多个其他组织进行敏感信息[1)]通信时,对敏感信息在其他组织中的使用将受到接收组织实现的充分安全控制的保护,发起方必须有信心。这可通过信息共享团体的建立来达到。信息共享团体中,虽然成员组织之间可能存在竞争,但每个成员仍信任其他成员会保护已共享信息。

只有建立了信任的信息共享团体才能有效运行。信息提供方必须能够信任接收方不会泄露或不当的使用数据。同时,基于发起方给出的所有资质,信息接收方必须能够信任信息是准确的。以上两个方面都很重要,它们必须得到明确有效的安全策略和良好实践应用的支持。为达到此目标,所有团体成员必须实现一个涵盖已共享信息安全的通用管理体系,即信息共享团体的信息安全管理体系(ISMS)。

此外,在并不是所有接收方都将为发起方所知的信息共享团体之间,也可进行信息共享。如果在这些团体及其信息共享协议之间建立起充分的信任,这种信息共享将可进行。特别相关的是在不同团体之间(如不同产业或市场行业)共享敏感信息。

本标准提供了使用已建立的通讯和其他技术方法如何满足规定要求的指南和通用原则。其目的是支持在交换和共享敏感信息时创建信任,从而促进信息共享团体的国际化发展。

标准中“针对行业间和组织间通信没有附加的信息”,指的是 GB/T 22081—2008 中对应条款没有附加的信息。

本标准题目中“通信”主要是指进行信息交换与共享,包括书面、口头、电子等所有形式信息交换与共享。

1）　行业或组织认为可能造成利益损失但又不能成为国家秘密的信息为敏感信息。

信息技术　安全技术　行业间和组织间通信的信息安全管理

1　范围

本标准给出了信息安全管理体系(ISMS)标准族的补充指南,用于在信息共享团体中实现信息安全管理。

本标准特别为组织间和行业间通信给出了有关发起、实现、维护与改进信息安全的控制和指南。

本标准适用于行业间各种公共和私有的、国内的和国际的所有形式的敏感信息交换与共享。特别是,本标准可适用于与组织或国家关键基础设施的供给、维护和保护相关的信息交换与共享。

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 22080—2008　信息技术　安全技术　信息安全管理体系　要求(ISO/IEC 27001:2005,IDT)

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 29246—2012　信息技术　安全技术　信息安全管理体系　概述和词汇(ISO/IEC 27000:2009,IDT)

3　术语、定义和缩略语

3.1　术语和定义

GB/T 29246—2012 界定的以及下列术语和定义适用于本文件。

3.1.1

信息共享团体　information sharing community

商定共享信息的组织群。

注:组织可以是个体。

3.1.2

可信信息通信机构　trusted information communication entity

信息共享团体内支持信息交换的自治组织。

3.2　缩略语

下列缩略语适用于本文件:

CVE	公共漏洞和暴露	(Common Vulnerabilities & Exposures)
IPR	知识产权	(Intellectual Property Right)
ISIRT	信息安全事件响应组	(Information Security Incident Response Team)
ISMS	信息安全管理体系	(Information Security Management System)
P2P	对等通信	(Peer to Peer)