互联网信息服务内容安全要求及评估框架研究

王宇航[1,2], 郭 涛[1,2], 张潇丹[1,2], 孟 丹[1,2], 韩冀中[1,2], 周 熙[1,2]

[1] 中国科学院信息工程研究所 北京 中国 100093
[2] 中国科学院大学网络空间安全学院 北京 中国 100049

摘要 互联网的飞速发展带来信息内容的爆炸式增长, 对互联网信息安全特别是信息内容安全治理提出了更高挑战。互联网新技术、新应用的发展深刻改变了互联网信息的传播方式, 在极大推动数字信息增长和全球化一体化发展的同时, 也为各种错误的、歪曲的、低俗的、与社会主流价值观相违背的有害信息提供孕育、发酵、传播和驻留的温床。目前, 国内外信息技术/产品、信息系统的安全要求和评估方法, 已形成了较为成熟的体系。但是, 已有信息安全风险评估模型和评估指标体系很少涉及信息内容安全, 专门针对互联网信息内容安全的通用要求和评估体系的研究在全球范围内尚为空白。本文在总结分析国内外已有成熟的信息安全评估标准基础上, 从信息论角度对信息空间进行了分层, 提出信息技术/产品安全、信息系统安全、信息服务安全三个层次的网络空间安全体系, 主要借鉴信息技术安全评估通用准则(ISO/IEC 15408)、信息系统安全保障评估框架(GB/T 20274)等标准设计思路, 结合我国互联网信息服务特点、安全现状及发展趋势, 深入分析了信息内容安全风险要素之间的关系, 提出一套以互联网信息服务为评估对象的安全评估通用要求模型及评估框架。上述模型框架具有良好的可扩展性, 可面向不同形式的信息服务编制保护轮廓和安全目标并实施安全评估, 为互联网新兴技术应用的安全发展需要和监督管理需求提供了良好的技术基础支撑。相关成果编制为国家推荐性标准, 具有一定的先进性和可操作性。

关键词 信息安全; 信息内容安全; 信息服务; 安全要求; 安全评估
中图法分类号 TP309.2 DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.01.02

Security Requirements and Evaluation Framework for Internet Information Service Content

WANG Yuhang[1,2], GUO Tao[1,2], ZHANG Xiaodan[1,2], MENG Dan[1,2], HANG Jizhong[1,2], ZHOU Xi[1,2]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract The rapid development of the Internet has brought about the explosive growth of information content, which poses higher challenges to Internet information security, especially information content security governance. The development of new Internet technologies and new applications has profoundly changed the way Internet information is disseminated. While greatly promoting the growth of digital information and the development of globalization, it has also provided a ground of breeding, fermentation, dissemination and residence for various wrong, distorted, vulgar, and mainstream social values. At present, the security requirements and evaluation methods of information technology/products and information systems at home and abroad have formed a relatively mature system. However, the existing information security risk assessment models and assessment index systems rarely involve information content security, and the research on general requirements and assessment systems specifically for Internet information content security is still blank on a global scale. Based on the summary and analysis of mature information security assessment standards at home and abroad, this paper has carried out a layered analysis of information space from the perspective of information theory, and proposed a cyberspace security system with three levels of information technology/product security, information system security, and information service security. Learning from the standard design ideas of common criteria for information technology security assessment (ISO/IEC 15408) and framework of information system security assurance assessment (GB/T 20274), and combining with the characteristics of China's Internet information services, security status and development trends, we deeply analyzed the relationship between risk elements of information content security, and proposed a set of general requirements model and evaluation framework for Internet information services. The above model framework has good scalability, can prepare protection profiles and security goals and implement security assessments for different forms of information services, providing a good technical foundation for the needs of security development and supervision and management for emerging Internet technology applications. The relevant results have been compiled as advanced and operable national recommended standards.

通讯作者: 郭涛, 博士生导师, 研究员, 工学博士, Email: guotao@iie.ac.cn。

本课题得到 2018 年度互联网新技术新应用安全评估与标准体系研究项目(No. Y8V0971105)、信息安全技术互联网信息安全服务通用要求(No. Y9V1301、No. 90SNHTBH-2019111326)资助。
收稿日期: 2020-05-03; 修改日期: 2020-07-03; 定稿日期: 2021-11-22

erable national recommended standards.

Key words information security; information content security; information service; security requirements; security evaluation

1 引言

近年来, 人工智能、区块链、5G、个性化推荐算法等前沿技术飞速发展, 互联网用户不断增加, 网络结构日趋庞大复杂, 网上数字信息呈爆发式增长, 即时通讯、网络直播、短视频等新型信息服务不断涌现[1]。互联网新技术、新应用的发展深刻改变了互联网信息的传播方式[2], 在极大推动数字信息增长和全球化一体化发展的同时, 也为各种错误的、歪曲的、低俗的、与社会主流价值观相违背的有害信息提供孕育、发酵、传播和驻留的温床[3]。由于互联网新技术、新应用发展异常迅速, 互联网信息服务往往采用“小步快跑, 多次迭代”的开发模式, 很多信息服务在功能设计或实现上都存在大量缺陷, 导致信息内容安全问题日益严峻。

传统网络安全主要关注信息技术/产品、信息系统的安全防护[4-6], 在互联网信息服务海量增长, 有害信息扩散和蔓延趋势日益严重的情况下, 传统的信息技术安全评估体系已无法满足互联网信息安全防护的迫切需要[7]。目前, 国内外互联网信息安全研究主要集中于数据采集[8]、存储[9]和跨境流动[10]等方面, 对于信息内容本身的合理合规生产和使用研究较少。国内互联网信息内容安全实践处于起步阶段, 相关立法情况薄弱, 仅在《中华人民共和国网络安全法》(以下简称《网络安全法》)《互联网信息服务管理办法》《网络信息内容生态治理规定》等法律法规和少量部门规章的部分条款中做出较为宽泛模糊的规定[11]; 相关国家标准和行业标准不足, 截至 2020 年 4 月, 仅有《互联网信息服务安全通用要求》[12]一项国标在研。互联网信息内容层面安全评估手段的缺失, 成为了一项亟待解决的问题。风险评估是保障信息安全的一项成熟关键技术[13], 对互联网信息服务开展安全风险评估是一种从源头遏制有害信息产生和扩散的有效做法。

本文首先从信息论角度对信息空间进行了分层, 将网络空间安全划分为信息技术/产品安全、信息系统安全、信息服务安全三个层次, 总结分析了国内外成熟的信息安全评估标准。借鉴信息技术安全评估通用准则(ISO/IEC 15408)、信息系统安全保障评估框架(GB/T 20274)等标准设计思路, 结合我国互联网信息服务特点和安全风险现状及趋势, 在充分调研基础上, 提出一套以信息服务为具体评估对象的互联网信息服务安全评估要求模型及评估框架。相关成果正在编制国家推荐性标准, 具有一定的先进性和可操作性。

2 信息安全评估概述

2.1 网络空间安全与信息安全

在经历了机械化、电气化之后, 人类社会进入了信息化时代, 信息和信息技术极大改变了人们的工作和生活, 信息已经成为基础资源之一, 有的国家已将其当作一种战略资源[14]。从本质上来说, 信息是事物的一种属性[15], 信息表达需要借助约定的符号, 如文字、图形、音频、视频等, 信息的存储传播需要借助特定的载体介质, 如纸张、磁盘、光盘、电信网络线路等。人们创造 Cyberspace 一词以刻画人类生存的信息空间环境, 但对其尚无统一定义。该词在我国的译名也不统一, 张焕国等[16]认为, Cyberspace 是“信息时代人们赖以生存的信息环境, 是所有信息系统的集合”, 可翻译为“信息空间”或“网络空间”, 前者突出信息这一核心内涵, 后者突出网络互联这一重要特征。2015 年 12 月, 习近平总书记在第二届世界互联网大会开幕式上发表主旨演讲, 就共同构建网络空间命运共同体提出 5 点主张。至此, “网络空间”的说法成为主流。

安全与信息相伴相生, 就像信息的影子, 哪里有信息哪里就存在安全问题。自 20 世纪 90 年代互联网蓬勃发展开始, 信息的安全问题日益获得世界各国广泛关注, 在不同历史阶段出现过不同的概念和分类: 通信安全(COMSEC: Communication Security)、计算机安全(COMPUSEC: Computer Security)、信息技术安全(INFOSEC: Information Technology Security)、信息系统安全保障(IA: Information Assurance)等[17]。国际信息系统安全认证协会(ISC)认为信息安全包括物理安全、通信和网络安全、密码学等 10 个领域[18]。上海社会科学院编撰的《信息安全词典》[19]对信息安全的定义为: “保障国家、机构、个人的信息空间、信息载体和信息资源不受来自内外各种形式的危险、威胁、侵害和误导的外在状态和方式及内在主体感受”。《网络安全法》[20]将网络安全分为网络运行安全、网络信息安全。张焕国等在《网络空间安全综述》[16]中指出, “信息系统安全

划分为 4 个层次: 设备安全、数据安全、内容安全、行为安全, 其中数据安全即是传统的信息安全”。

从信息论角度来看, 网络空间中的信息技术/产品、信息系统、信息服务是信息的载体, 信息数据和信息内容是信息的本质内涵[16]。网络空间通常可根据不同的信息载体划分为以下三个层次。最上层是信息服务, 重点面向信息内容提供服务。对互联网用户而言, 创作或访问信息内容的信息服务主要由 Office、WPS 等文字处理软件, 酷狗音乐、暴风影音等多媒体播放器, IE、Firefox、Chrome 等网页浏览器, 微信、新浪微博、今日头条、抖音等应用程序提供; 信息内容的表现形式主要包括: 文字、图片、音频、视频、关联关系等; 对平台运营者而言, 可提供信息服务的方式包括互联网站、应用程序、轻应用等。中间层是信息系统, 指的是用于采集、处理、存储、传输、分发和部署信息数据的整个基础设施、组织结构、人员和组件的总和[21]。最底层是构建信息系统的信息技术/产品, 即路由器、防火墙、服务器、操作系统、数据库等“砖块瓦片”。因此, 网络空间安全主要包括: 信息技术/产品安全、信息系统安全、信息服务内容安全, 网络空间安全的重中之重是信息服务内容安全。

2.2 信息技术/产品安全评估

信息安全是信息化持续发展的根本保障, 信息安全评估是信息安全保障工作的基础性工作和重要环节[14]。信息安全评估是指依据有关安全技术与管理标准规范, 对信息载体及由其处理、传输和存储的信息, 进行保密性、完整性、可用性等安全属性的科学评价过程[22]。

国际上信息技术/产品安全评估标准化工作起源于 20 世纪 70 年代中期, 80 年代有了较快发展, 90 年代引起了世界各国的普遍关注, 至今已经形成了较为完备的信息技术安全标准体系[23]。主要包括三个里程碑式的标准: TCSEC、ITSEC 和 CC。

1985 年, 美国国防部发布《可信计算机系统评估准则》(TCSEC, 桔皮书)[24], 主要针对计算机操作系统开展安全评估, 重点关注保密性。1991 年, 西欧四国(英、法、德、荷)联合提出了《信息技术安全评估准则》(ITSEC)[25], 在关注保密性基础上, 增加了对完整性、可用性要求, 并将安全要求划分为“功能”和“保障”两部分, 功能指的是为满足安全要求而采取的一系列技术安全措施, 保障指的是确保功能正确实现及有效性的安全措施。

为满足全球经济信息化发展的需要, 减少各国信息安全测评认证的重复开支, 国际上希望建立一套统一的信息技术安全评估标准。1996 年, 美国、加拿大等六国七方签署了《信息技术安全评估通用准则》(CC v1.0), 后续经不断完善, 最新版本为 CC v3.1。1999 年, CC v2.0 被采纳为国际标准, 最新版是 ISO/IEC 15408-2009[26]。自从 CC 及其相关标准问世以来, 很多国家相继采用或借鉴其准则条例, 以实施本国的信息技术/产品安全评估与认证。目前全球已经有 17 个国家签署了《通用准则国际互认协定》(CCRA), 并另有 14 个国家认可 CC 认证结果。

我国信息安全管理与国际基本同步。1994 年中国首次接入国际互联网后, 相继出台《中华人民共和国计算机信息系统安全保护条例》等一系列面向信息技术安全保护方面的法律法规和国家标准。1999 年, 我国将 TCSEC 转化为国家标准《计算机信息系统安全防护等级划分准则》(GB 17859-1999)[27]。2001 年, 我国将国际标准 ISO/IEC 15408-1999 等同采用为国家推荐性标准《信息技术安全评估准则》(GB/T 18336-2001)[28-29], 最新升级为 GB/T18336-2015[30]。2007 年, 国家发布《信息安全风险评估规范》(GB/T 20984)[22], 提出风险评估的概念、要素关系、评估原理、实施流程和工作方法等, 用于规范化风险评估过程。2017 年 6 月《网络安全法》正式施行, 作为我国网络安全领域的基础性法律, 全面规范了网络空间主权、关键信息基础设施安全保护、重要数据本地化储存、个人信息保护等网络空间治理关键领域的基本框架。

2.3 信息系统安全评估

信息技术/产品安全是信息安全的基础, 随着互联网飞速发展和信息技术/产品功能复杂化, 由大量多类型、多品种的信息技术/产品及其运行环境构成的信息系统所面临的信息安全风险远远超出了信息技术/产品本身[31], 不再仅局限于计算机设备和网络等信息载体, 对于信息载体所处的物理环境、人员管理、使用过程等同样提出了安全要求, 国内外也相继从管理角度提出了信息系统安全管理标准。

1995~1998 年, 英国标准协会(BSI)发布《信息安全管理实施规则》(BS 7799-1)[32]和《信息安全管理体系规范》(BS 7799-2)[33], 后被采纳为国际标准《信息安全管理实施规则》(ISO/IEC 17799-1)[34]和《信息安全管理系统要求》(ISO/IEC 27001)[35], 最新版本分别为 ISO/IEC 27002-2013[36]和 ISO/IEC 27001-2013。其中, 《信息安全管理实施规则》是组织建立并实施信息安全管理体系的指导性准则, 为组织制定自身信息安全策略、进行有效信息安全控制提供依据; 《信息安全管理体系规范》提供一套有效的信息安

全管理体系模型以及信息安全控制要求。

1996 年, 美国国家安全局(NSA)开发一套专门用于系统安全工程的信息安全工程能力成熟度模型(SSE-CMM), 基于众多软件专家的实践经验, 侧重于软件开发过程的管理和工程能力的提高与评估[17]。2002 年, SSE-CMM 被国际标准化组织采纳为国际标准《信息技术系统安全工程－成熟度模型》(ISO/IEC 21827-2002), 最新版本为 ISO/IEC 21827-2008[37]。

1996 年, 国际标准化组织(ISO)发布《信息安全管理指南》(ISO/IEC TR 13335)[38], 提供了一套以风险为核心的信息安全管理模型, 以给出具体信息安全管理建议和指南为目标, 从多种角度阐述信息安全管理模型并给出操作性较强的步骤。

2006 年, 我国发布国家标准《信息系统安全保障评估框架》(GB/T 20274)[21], 将评估对象从 GB/T 18336 的信息技术/产品, 扩展到包括基础设施、组织结构、人员和组件等总和的信息系统, 提出信息系统安全保障策略体系, 从安全技术、安全工程和安全管理等方面提出安全保障要求。

3 信息内容安全评估

3.1 信息内容安全

西方国家对网络信息安全的重视始于 20 世纪 90 年代, 侧重于信息载体安全和信息数据安全, 对信息内容安全管理基本奉行“言论自由”。自 2001 年“9·11”事件中恐怖分子利用互联网传递信息策划恐怖活动, 并对国际安全造成严重损害后, 以美国为首的西方国家开始将信息安全的范围和重心逐步扩大到信息内容安全[39]。

国际上有诸多面向特定领域的信息内容安全法律准则, 在国际公约方面如 1910 年管制色情的《反对传播淫秽出版物协定》, 1948 年查禁民族仇杀内容的《防止和惩罚民族屠杀公约》, 1966 年禁止宣传战争的《联合国人权宣言》; 在各国法律法规中, 如美国在 1996 年颁布针对网络色情内容的《传播净化法案》, 1998 年和 2000 年颁布针对儿童网络内容安全的《儿童在线保护法》和《儿童网上隐私保护法》, 2001 年颁布针对通信内容安全的《通信规范法案》, 日本在 2008 年颁布针对未成年人网络内容安全的《约会类网站规制法》和《青少年网络环境整备法》等等。此外, 在制度上, 美国要求学校必须安装过滤系统以保证校园网内不能访问违法信息, 对互联网信息内容进行分级, 对互联网信息内容受众进行分类; 意大利采用了微软互联网儿童色情屏蔽系统; 日本施行电子娱乐信息内容分级制度; 韩国对手机邮件采取集中控制, 通过技术手段拦截有害邮件; 新加坡施行互联网分级许可证制度, 建立信息关防封堵色情信息等。

2000 年, 我国颁布《互联网信息服务管理办法》(国务院第 292 号令)[40], 对从事互联网信息服务的主体明确规定了取得许可和备案义务, 信息内容安全逐步获得国家和行业层面的关注。2017 年, 我国颁布《网络安全法》, 明确信息内容安全属于信息安全范畴。信息内容安全已然成为了国家信息安全保障体系的重要组成部分[41]。

由于国内外在信息内容安全管理领域仍处于起步探索阶段, 目前针对信息内容安全要求的刻画, 缺乏标准化、规范化的公共描述语言、结构和方法, 仅在个别法律法规和标准中有“枚举式”表述。

例如, 在法律法规方面, 我国《互联网信息服务管理办法》第十五条指出, 互联网信息服务提供者不得制作、复制、发布、传播含有“九不准”内容的信息; 国家广播电影电视总局、中华人民共和国信息产业部颁布的《互联网视听节目服务管理规定》[42](第 56 号令)第十六条指出视听节目不得含有的 10 项内容; 国家广播电影电视总局颁布的《广电总局关于加强互联网视听节目内容管理的通知》[43]第二节指出视听节目应及时剪节、删除的 21 项内容, 《电视剧内容管理规定》(第 63 号令)[44]第五条指出电视剧不得载有的 11 项内容; 中国网络视听节目服务协会颁布的《网络视听节目内容审核通则》[45]第四章“节目内容审核标准”中, 列举了互联网视听节目不得出现的 4 条 47 款共计 109 项内容, 《网络短视频内容审核标准细则》[46]中列举了网络短视频不得出现的 21 条共计 100 项内容, 《网络综艺节目内容审核标准细则》[47]中列举了网络综艺节目不得出现的 2 部分 9 类共计 94 条内容; 在 2013 年国家互联网信息办公室举办的“网络名人社会责任论坛”上, 由网络名人达成共识, 提出的网友应遵守的“七条底线”原则等。

在国家和行业标准方面, 国家标准《信息安全事件分类分级指南》(GBZ 20986-2007)[48]将信息内容安全事件定义为: “利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件”。工业互联网安全[49]方面的规划主要集中在设备安全、控制系统安全、网络安全等; 在新技术新形态领域如 5G 通信[50,51]、区块链[52]等方面的国家和行业标准尚处于起步规划阶段, 安全要求方面目前聚焦于网络安全、技术安全和设备安全, 涉及信息内容安全较少。

根据上述国内外法律法规和国家标准中对互联网信息内容安全的相关规定, 本文将信息内容安全定义为对信息的内容真实有效, 符合法律法规、社会公德、商业道德的保护。

3.2 信息内容安全评估

信息安全评估的基本思路是通过对信息技术、产品、系统等的风险分析挖掘, 提出对应的安全保障要求, 识别并改进信息产品脆弱性, 使其在期望的安全环境中运行, 减少信息安全风险, 保障资产安全[31]。在众多信息安全模型[21,26,35,38]中, “风险”始终是占据关键位置的核心要素, 风险评估和管理具有重要性、基础性作用。图 1 说明了信息安全各要素的关系。资产是赋予了价值的实体, 对于所有者和威胁主体都具有价值, 所有者有责任保护资产利益不降低, 威胁主体希望以危害资产所有者利益的方式非法获取或破坏资产, 威胁引发了资产的安全风险, 威胁主体可利用已有威胁实现其目的, 所有者希望通过实施对策降低风险, 保护信息资产安全。

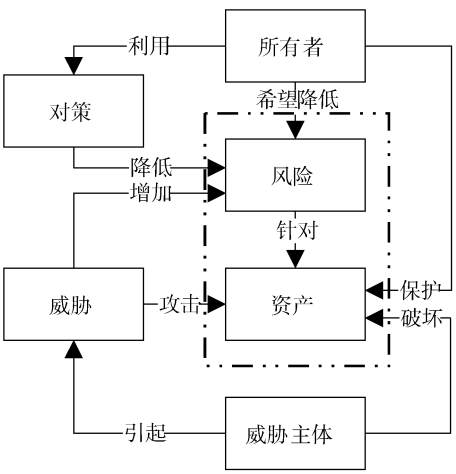

图 1 信息安全风险要素关系

Figure 1 Relationship among elements of information security risks

在信息技术/产品安全中, 信息一般认为应具有 CIA 三个安全属性: 机密性(Confidentiality)确保信息不被泄露, 完整性(Integrity)确保信息不被篡改, 可用性(Availability)确保信息可被合法使用[53]。在信息系统安全中, 通常还会补充考虑以下安全责任属性: 如可控性确保信息传播可被控制, 可确认性确保信息不可抵赖, 可审计性确保信息可被溯源等[31]。在信息内容安全层面, 信息还应具有真实性、优良性, 以确保信息内容符合事实, 符合法律法规、社会公德、商业道德等。

在传统信息安全范畴中, 信息技术/产品安全和信息系统安全风险关系模型已十分成熟。对于信息技术/产品安全来说, 资产是信息及信息技术/产品, 其实现形式可以是硬件、固件或软件, 威胁可以是信息技术/产品漏洞[30], 已有对策包括实施 CC、GB/T 18336 等, 以确保信息的 CIA 安全属性。对于信息系统安全来说, 资产是信息及整个基础设施、组织结构、人员和组件等总和的信息系统[21], 威胁可以是信息系统在技术、人员管理等方面的漏洞, 已有对策包括实施 GB/T 20274 等, 除确保信息的 CIA 安全属性外, 还应确保信息的安全责任属性[31]。图 2 描述了上述风险要素层次关系。

对于信息服务安全来说, 所有者是信息服务提供者, 资产是信息及提供信息内容的信息服务。随着互联网新技术的深入发展和网民对信息交流方式多样化的迫切需要, 互联网信息服务形式和功能日趋丰富繁杂, 个性化新闻资讯推荐、网络直播互动、群组视频通信、匿名社交、换脸变声、虚拟现实影像等新功能推陈出新, 不断对互联网信息内容安全带来新的威胁。对于互联网信息服务, 威胁可以是内容审核机制缺失漏洞、采编人员管理漏洞等, 威胁主体可以是发布虚假信息的恶意用户、采编有害稿源的编辑、推送低质庸俗信息的个性化推荐算法等。资

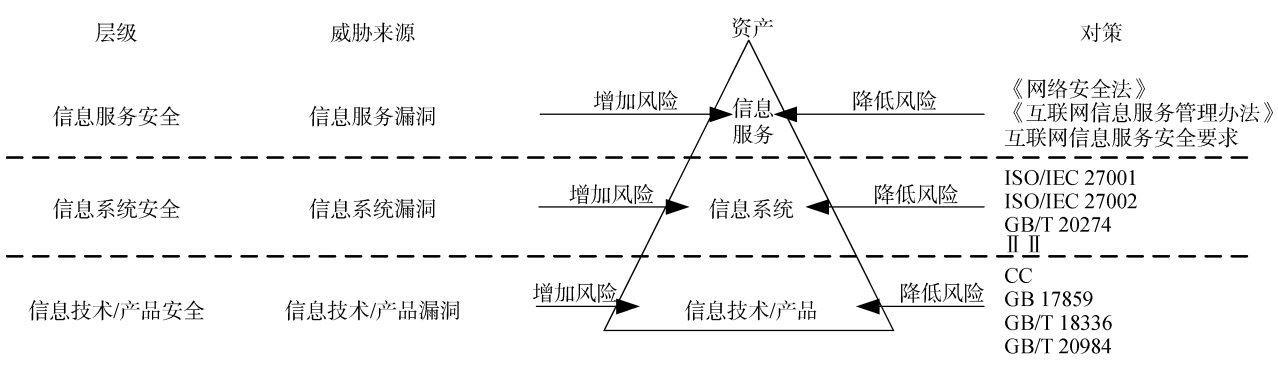

图 2 分层次的信息安全风险要素举例

Figure 2 Examples of elements of hierarchical information security risks

产对所有者和威胁主体都具有价值, 信息服务提供者通过信息服务提供信息内容, 创造商业利益, 威胁主体利用信息服务内容审核管理漏洞等实现散布有害信息等恶意目的, 危害信息服务安全。

与信息技术/产品安全评估、信息系统安全评估相同, 对信息服务实施安全评估管理, 需要先定义安全行为准则[54], 并制定安全防护措施、安全评测评估和安全审查认定方法, 管理部门依据安全行为准则和评估方法实施安全评估和有效监督管理。由于目前信息服务安全评估方面顶层设计不足, 尚无可具体指导实施安全防护措施的国家标准和操作指南等, 许多互联网信息服务在经过传统信息安全评估或检查手段之后, 在已满足特定级别等级保护要求的情况下, 仍然频繁发生严重信息内容安全事故。

信息技术/产品安全评估的评估对象(Target of Evaluation, TOE)为软件、固件、硬件和指南文件的集合[30], 信息系统安全评估的 TOE 为提供信息采集、处理、存储、传输、分发和部署等技术或功能的信息系统[21], 信息服务安全评估的 TOE 为提供信息生成、处理、使用、传播、存储和销毁等技术或功能的信息服务。本文借鉴信息技术安全评估通用准则(ISO/IEC 15408)、信息系统安全保障评估框架(GB/T 20274)等已有信息安全风险评估实践的设计理念, 将 TOE 扩展为提供信息内容的互联网信息服务, 提出互联网信息服务内容安全要求, 并以结构化方式对信息服务内容安全要求和安全评估要求进行描述, 为互联网信息服务相关方提供安全保障工作参考。

4 互联网信息服务内容安全要求

《互联网信息服务管理办法》第 2 条将互联网信息服务定义为“通过互联网向上网用户提供信息的服务活动”, 其服务形式多样, 如根据 2017 年国家互联网信息办公室令第 1 号《互联网新闻信息服务管理规定》[54]第 5 条的列举, 服务形式包括互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等。本文认为互联网信息服务是一种基于信息生成、处理、使用、传播、存储和销毁等技术或功能, 通过互联网提供信息的服务活动。

CC 的目标是建立一套完备的对信息系统和应用安全性进行评估所需的标准化基础准则, 针对在安全评估过程中信息系统和应用的功能安全性和相应的保障措施, 提出一组通用要求, 以使各独立的安全评估结果具有可比性[55]。对于信息内容安全管理, 互联网信息服务的相关方(所有者、使用者或评估者), 同样需要一种标准化、规范化的公共描述语言、结构和方法, 以描述该信息服务在信息内容安全方面应该达到的通用要求, 并使用这种公共语言与信息服务的其他相关方进行沟通。

信息服务的所有者可参照此要求, 根据其在信息服务全生命周期中的角色完成相应工作, 即设计、实现或运维相应的安全措施, 降低信息服务可能产生的信息内容安全风险。信息服务评估者可参照此要求, 使用科学规范的评估方法对信息服务已采取的安全措施进行评估, 研判相关措施是否满足相应安全要求; 评估者通过评估所得到的客观证据, 增强信息服务使用者和其他相关方对信息服务在其运行过程中对抗威胁、保护资产和实现使命的信心。同时, 信息服务相关方应在信息服务全生命周期中持续改进和完善保障措施, 形成可持续改进的信息服务安全保障能力, 维护信任。

4.1 模型概述

本文调研了国内主要互联网信息服务, 包括苹果 APP Store、华为、小米和豌豆荚等国内主流应用商城的下载量总和排名前 600 名的信息服务; 同时, 为重点关注新闻信息服务, 增加调研国家互联网信息办公室 2016 年底发布的 293 家互联网新闻信息服务网站, 服务形式涵盖了即时通讯、论坛博客、搜索引擎、网络直播等。在深入分析各功能含义和差异的基础上, 基于信息生命周期, 将信息服务的主要功能归纳为信息发布、信息分享、评论评价等 16 类, 其中“非提供信息的功能”包括输入法、网络资源管理、设备管理等。图 3 显示了上述 893 个信息服务面向用户提供功能的情况。

信息服务安全性有两个重要度量维度: 一是所能提供的安全功能, 二是安全功能的可信度。因此, 信息内容安全要求也分为安全功能要求和安全保障要求两类, 前者用于描述产品应该提供的安全功能, 后者用于描述安全可信度以及为获取一定可信度应该采取的安全措施。二者应尽可能相互独立。

本文提出互联网信息服务内容安全评估模型(图 4), 以安全工程思想为指导, 按照信息服务生命周期线索, 将各类互联网信息服务的功能模块归类分析, 提出安全功能要求和安全保障要求两类信息内容安全要求, 以定义期望的安全行为和保证安全措施正确有效实施的信任基础。在安全要求的表达上, 以组件化描述方式通过类、族和组件 3 级层次结构对信息服务安全要求进行描述。

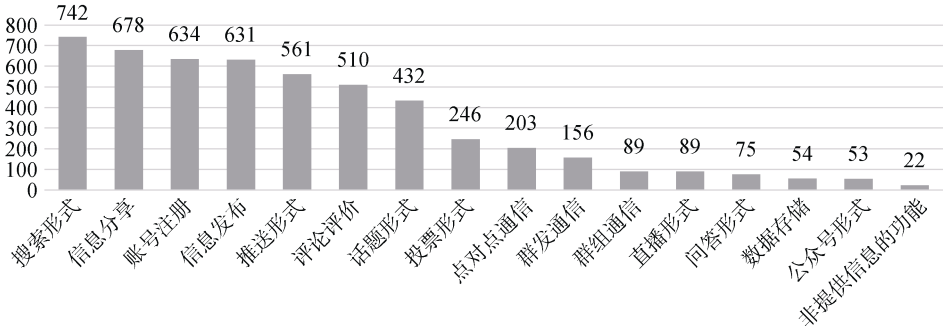

图 3　893 款互联网信息服务功能分布情况

Figure 3　Distribution of 893 Internet information services

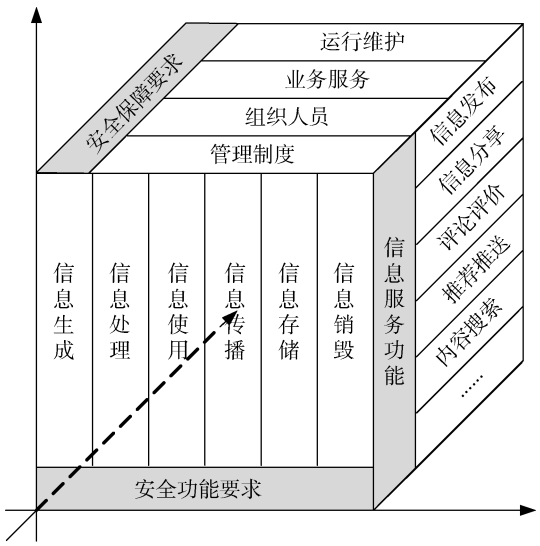

图 4　互联网信息服务内容安全评估模型

Figure 4　Model of evaluation for Internet information service content security

在类层面, 根据信息在不同生命阶段的安全问题, 将安全要求全集划分为若干类; 在族层面, 将每个安全要求类根据不同安全目标, 划分为若干族; 在组件层面, 将每个安全目标族进一步划分为具有原子性的组件, 以供进行安全运营或风险评估等活动时选用。类和族体现的是一种分类方法, 具体的安全要求由组件体现, 即每一个信息服务的安全目标都可以通过最小可选组件描述。通过选取安全功能组件描述信息服务提供功能应满足的安全行为, 选取安全保障组件描述上述安全行为正确有效实施的保障要求。通过安全功能组件和安全保障组件构造用于描述某种服务功能安全目标的组件包、某一类信息服务安全目标的保护轮廓(Protection Profiles, PP)文档, 由此构造描述特定信息服务的安全目标(Security Target, ST)文档。本文通过对 893 款互联网信息服务各项功能的逐一分析, 验证了上述模型可满足对互联网信息服务应提供的安全功能描述。

4.2　安全组件

互联网上信息内容安全风险来自多个方面, 如信息服务提供者从不合规稿源采集虚假信息、提供信息服务时未对用户上传的违法不良信息有效拦截、信息内容发布流程多级审核机制不健全、已发布信息巡查不及时、用户信息存储未配备有效防篡改技术措施、信息销毁不彻底等。本文参考国际标准化组织 ISO/TC171 相关决议[56]、美国学者 Horton[57]对信息生命阶段在两个层面上的定义和我国学者索传军[58]对信息生命阶段的界定等研究, 将互联网信息服务提供的信息活动分为 6 个阶段: 信息生成、信息处理、信息使用、信息传播、信息存储和信息销毁。

在互联网信息服务内容安全评估模型中, 安全功能要求按照信息生命周期设置为信息生成等 6 类, 根据不同的安全目标下设安全功能要求族, 进而再设计更为具体的安全功能要求组件, 具体结构见表 1。安全保障要求设置管理制度、组织人员、业务服务和运行维护 4 类, 并依据不同保障目标下设安全保障要求族和安全保障要求组件, 具体结构见表 2。

4.3　安全等级分级

由于互联网信息服务的功能类型、信息形式、服务用户规模不同, 信息服务的社会动员能力也不同。在互联网信息服务内容安全评估模型中, 对于具有不同社会动员能力的信息服务采取了安全等级分级策略。模型将互联网信息服务安全初步划分为基本级和增强级, 从所属企业规模、服务用户规模、提供信息形式 3 个要素, 判断该互联网信息服务的社会动员能力和发生安全事件后的危害程度, 从而确定其应满足的安全级别, 为评估者提供分级的安全要求依据。具体分级规则见表 3。

表 1　安全功能组件

Table 1　Security functional components

类	族	组件
A.1: 信息生成	A.1.1: 信息采编	A.1.1.1: 信息源规范、A.1.1.2: 信息采编规范、A.1.1.3: 信息源追溯
	A.1.2: 信息生成主体	A.1.2.1: 信息服务用户注册、A.1.2.2: 信息生成主体保护、A.1.2.3: 信息生成主体溯源
A.2: 信息处理	A.2.1: 信息内容检测	A.2.1.1: 信息内容识别、A.2.1.2: 信息内容过滤、A.2.1.3: 信息内容人工审核
	A.2.2: 信息服务分级分类	A.2.2.1: 信息内容分级、A.2.2.2: 信息内容分类、A.2.2.3: 用户账号分级、A.2.2.4: 用户账号关联
A.3: 信息使用	A.3.1: 发布信息	A.3.1.1: 信息发布策略、A.3.1.1: 信息发布管理
	A.3.2: 使用信息	A.3.2.1: 用户使用信息策略、A.3.2.2: 用户使用信息管理
A.4: 信息传播	A.4.1: 信息安全监测预警	A.4.1.1: 信息安全监测巡查、A.4.1.2: 信息安全预测告警、A.4.1.3: 投诉举报管理
	A.4.2: 信息安全事件处置	A.4.2.1: 信息安全事件分级分类、A.4.2.2: 信息安全事件响应处置、A.4.2.3: 配合监督管理
A.5: 信息存储	A.5.1: 系统信息	A.5.1.1: 日志记录规范、A.5.1.2: 日志存储管理
	A.5.2: 服务信息	A.5.2.1: 采编信息、A.5.2.2: 用户账号信息、A.5.2.3: 样本库信息、A.5.2.4: 意见投诉信息、A.5.2.5: 安全事件信息、A.5.2.6: 配合监管信息
A.6: 信息销毁	A.6.1: 销毁信息	A.6.1.1: 信息销毁策略、A.6.1.2: 用户注销管理

表 2　安全保障组件

Table 2　Security assurance components

类	族	组件
B.1: 管理制度	B.1.1: 制度保障	B.2.1.1: 制度配备、B.2.1.5: 制度执行与管理
B.2: 组织人员	B.2.1: 组织机构	B.2.2.1: 管理机构、B.2.2.2: 管理人员
	B.2.2: 从业人员	B.2.2.2: 从业人员配备、B.2.2.3: 从业人员管理、B.2.2.4: 从业人员培训
B.3: 业务服务	B.3.1: 数据安全	B.3.1.1: 数据保护、B.3.1.2: 数据存储、B.3.1.3: 数据销毁
	B.3.2: 内容安全	B.2.1.2: 信息内容有效性、B.2.1.3: 信息内容安全性
B.4: 运行维护	B.4.1: 技术保障	B.2.4.1: 技术配备、B.2.4.2: 技术使用管理、B.2.4.3: 技术更新管理
	B.4.2: 设施保障	B.2.3.1: 设备配备、B.2.3.2: 设备安全运行管理
	B.4.3: 服务运营	B.4.3.1: 运营策略、B.4.3.2: 运营管理
	B.4.4: 外包服务管理	B.4.3.1: 外包服务管理

表 3　互联网信息服务安全等级分级规则

Table 3　Grading rules of security level of Internet information service

分级要素		基本级	增强级
所属企业规模	营业收入≤1000 万元	✓	
	营业收入＞1000 万元		✓
服务用户规模	用户数量≤100 万人	✓	
	用户数量＞100 万人		✓
提供信息形式	文本、图片	✓	
	音频、视频		✓

互联网信息服务内容安全评估模型在部分安全功能组件和安全保障组件中分别设置了基本要求和增强要求。例如, 在安全功能组件“A.1.2.1: 信息服务用户注册”中, 基本要求定义了互联网信息服务的用户注册功能应满足与用户签订使用协议、用户填报信息先审后发、对问题账号及时处置 3 项要求, 增强要求增加定义了具备真实身份信息核验能力等。安全等级为基本级的互联网信息服务应满足所选组件中所有的基本要求, 安全等级为增强级的应同时满足所选组件中的基本要求和增强要求。

4.4　一致性分析

信息安全评估是在 TOE 的整个生命周期中, 通过风险分析, 依据评估要素制定相应安全评估策略, 从而确保信息安全。表 4 列出了信息技术/产品安全评估、信息系统安全评估和信息服务安全评估的三个关键要素: 从信息的安全属性上看, 三者对于保障的信息安全属性逐步增加, 这与三者保障信息安全的层次递进关系一致; 从 TOE 生命周期来看, 3 者关注的 TOE 不同, 其生命周期也有所不同, 但保障 TOE 全生命周期安全这一目标是一致的; 从评估要素上看, 三者对于保障资产安全的技术、管理、人员 3 个主要方面是一致的。

信息服务安全评估与信息技术/产品安全评估、信息系统安全评估关注的 TOE 不同, 构造的 PP 也不

同。例如, 信息技术/产品、信息系统安全要求构造的 PP 有防火墙、智能卡、数据库、VPN 等, 而信息服务内容安全要求可构造的 PP 诸如即时通信工具、网络直播工具、博客、论坛等。

表 4 信息技术/产品安全评估、信息系统安全评估、信息服务安全评估的比较

Table 4 Comparison of evaluation for IT security, information systems security and information service security

	信息技术/产品安全评估	信息系统安全评估	信息服务安全评估
安全属性	机密性、完整性、可用性	机密性、完整性、可用性、可控性、可确认性、可审计性	机密性、完整性、可用性、可控性、可确认性、可审计性、真实性、优良性
生命周期	构造开发、交付使用、运行维护、测评分类	计划组织、开发采购、实施交付、运行维护、废弃	产生、处理、使用、传播、存储、销毁
评估要素	技术、管理、人员		

4.5 安全评估流程

对互联网信息服务实施安全评估主要包括以下步骤:

步骤 1: 制定安全目标(ST)

(1) 根据评估对象(TOE)的产品形态、服务形式和具体功能等, 确定 ST 应包含的安全功能组件和安全保障组件;

(2) 根据互联网信息服务安全等级分级规则, 确定 TOE 所属安全等级, 明确选取的组件中应包含的安全要求;

(3) 制定 ST。

步骤 2: 实施安全评估

(1) 组建评估队伍, 根据 ST 设计测评表, 拟定评估方案, 制订评估实施总体计划;

(2) 启动安全评估, 验证 TOE 是否满足 ST 所列安全要求; 若满足, 则该项安全评估结果为“通过”; 否则, 为“不通过”;

(3) 编制评估报告。

步骤 3: 形成评估结论

(1) 如果 TOE 评估的每一项评估结果均为“通过”, 则评估结论为“通过该安全等级的安全评估”;

(2) 如果 TOE 评估中包含评估结论为“未通过”的评估项, 且评估使用的安全等级不是最低级, 则降低 1 个安全等级, 重复步骤 1;

(3) 否则, 评估结论为“不通过”。

4.6 安全评估案例分析

本文选取国内知名度较高的某互联网新闻资讯聚合网站作为评估对象, 通过对其实施安全评估, 进一步说明互联网信息服务内容安全评估模型的使用方法。该 TOE 于 2013 年上线提供服务, 目前营业收入≤1000 万元, 用户数量≤100 万人, 提供的信息内容形式包括文本、图片、音频、视频, 因此安全等级定为增强级。该 TOE 提供网络新闻、站内新闻搜索(大家都在搜)、外部网站搜索、第三方平台分享和个人中心 5 项功能。通过逐项分析上述功能, 依据互联网信息服务内容安全要求制定 ST, 共包含 244 个安全组件。在第一轮安全评估(增强级)中, 评估结果为“通过”的安全组件有 210 个, “不通过”的有 34 个, 因此该 TOE 未能通过增强级的安全评估; 在第二轮安全评估(基本级)中, 全部 244 个安全评估组件的评估结果为“通过”; 因此, 该 TOE 的最终安全评估结论为“通过基本级安全评估”。评估结果示例见表 5, 其中括号中的分数表示“符合要求项目数/项目总数”。

5 总结

随着互联网技术飞速发展以及我国互联网与世界的进一步深度融合, 互联网有害信息问题日益尖锐, 对互联网信息内容安全评估与防范措施的研究工作将会更加重要和急迫。互联网信息服务内容安全要求和评估体系建设研究是一项长期性、持续性的工作。

本文通过借鉴信息技术安全评估通用准则(ISO/IEC 15408)、信息系统安全保障评估框架(GB/T 20274)等标准的设计思路, 针对互联网信息服务内容安全提出通用要求, 并设计了具体的安全功能要求和安全保障要求框架。互联网信息服务内容安全要求具有良好的可扩展性, 可面向不同形式的信息服务编制保护轮廓和安全目标并实施安全评估, 为互联网新兴技术应用的安全发展需要和监督管理需求提供了良好的技术基础支撑。相关研究成果已成功立项国家推荐性标准《互联网信息服务安全通用要求》, 目前已完成公开征求意见。

下一步研究工作包括: 对互联网信息服务内容安全功能要求进行细化, 从建立不同级别安全信心的角度对安全要求进一步分级, 面向实际需要建立

表 5　一款 TOE 在安全等级为“增强级”时的评估结果示例

Table 5　Evaluation result of a TOE with reinforced security level

服务功能	子功能	安全组件			评估结果
网络新闻 (110/137)	转载 (24/31)	A.1: 信息生成	A.1.1: 信息采编	A.1.1.1: 信息源规范	通过
				A.1.1.2: 信息采编规范	通过
				A.1.1.3: 信息源追溯	通过
			A.1.2: 信息生成主体	A.1.2.1: 信息服务用户注册	通过
				A.1.2.2: 信息生成主体保护	通过
				A.1.2.3: 信息生成主体溯源	不通过
				……	
			直播(22/29)		
			投票(24/31)		
			推荐(14/15)		
			评论(26/31)		
		大家都在搜(26/27)			
		外部网站搜索(27/27)			
		第三方平台分享(28/31)			
		个人中心(19/22)			

更为严谨的分级评估模型; 进一步跟踪归纳互联网新兴技术和信息服务的发展, 针对性地提出安全要求组件包和保护轮廓; 研究制订互联网信息服务安全评估指南, 研究自动化安全评估技术手段等。

致　谢　在此向本文成文中给予指导的老师、提供帮助的同学和给本文提出建议的评审专家表示感谢。

参考文献

[1] The 45th China Statistical Report on Internet Development, CNNIC, http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202004/P020200428596599037028.pdf, April 2020.

[2] Yi C Q. *Research on Mechanism of Information Dissemination Based on Social Network*[D]. Harbin: Harbin University of Science and Technology, 2013.
(易成岐. 社会网络的信息传播规律研究[D]. 哈尔滨: 哈尔滨理工大学, 2013.)

[3] Acceptance of online reports in February 2020, China Internet illegal information reporting center, http://www.12377.cn/txt/2020-03/06/content_41082393.htm, March 2020.

[4] Peng J, Gao J. Research on Computer Network Information Security and Protection Strategy[J]. *Computer & Digital Engineering*, 2011, 39(1): 121-124, 178.
(彭珺, 高珺. 计算机网络信息安全及防护策略研究[J]. *计算机与数字工程*, 2011, 39(1): 121-124, 178.)

[5] Hui Z B. Development of Domestic Information Security Researches—Based on the Literature Metrological Analysis and Content Analysis In the Core Journals of CNKI(1980-2010)[J]. *Library and Information Service*, 2012, 56(6): 14-19.
(惠志斌. 国内信息安全研究发展脉络初探——基于 1980—2010 年 CNKI 核心期刊的文献计量与内容分析[J]. *图书情报工作*, 2012, 56(6): 14-19.)

[6] Zhang H G, Wang L N, Du R Y, et al. Research on Information Security Discipline[J]. *Journal of Wuhan University* (*Natural Science Edition*), 2010, 56(5): 614-620.
(张焕国, 王丽娜, 杜瑞颖, 等. 信息安全学科体系结构研究[J]. *武汉大学学报(理学版)*, 2010, 56(5): 614-620.)

[7] Huang Q S, Li L Y. Overview on Information Content Security of Cyberspace[J]. *Journal of Information Security Research*, 2017, 3(12): 1115-1118.
(黄旗绅, 李留英. 网络空间信息内容安全综述[J]. *信息安全研究*, 2017, 3(12): 1115-1118.)

[8] Zhuang X. *Design and Implementation of Data Collection Agent In Unified Network Security Management*[D]. Wuhan: Central China Normal University, 2009.
(庄欣. 统一网络安全管理中数据采集代理的设计和实现[D]. 武汉: 华中师范大学, 2009.)

[9] Fu Y X, Luo S M, Shu J W. Survey of Secure Cloud Storage System and Key Technologies[J]. *Journal of Computer Research and Development*, 2013, 50(1): 136-145.
(傅颖勋, 罗圣美, 舒继武. 安全云存储系统与关键技术综述[J]. *计算机研究与发展*, 2013, 50(1): 136-145.)

[10] Hui Z B. *Research on Internet Firms Risk Management of Trans-Border Data Flows In the Data Economy Era*[D]. Nanjing: Nanjing University, 2018.
(惠志斌. 数据经济时代互联网企业跨境数据流动风险管理研究[D]. 南京: 南京大学, 2018.)

[11] Chen G F, Liao G W. On the security of network information content[J]. *Chinese Criminology Review*, 2016(2): 50-55.
(陈贵峰, 廖根为. 论网络信息内容安全的保障[J]. *犯罪研究*, 2016(2): 50-55.)

[12] Notice of the national standard 'information security technology Internet information service security general requirements' to solicit comments on the draft notice, National Information Security Standardization Technical Committee, http://www.iie.ac.cn/xwdt2020/ kydt2020/202012/t20201211_5816463 .html, Oct. 2019.

[13] Li H T, Liu Y, He D Q. Review on Study of Risk Evaluation for IT System Security[J]. *China Safety Science Journal* (*CSSJ*), 2006, 16(1): 108-113, 0.
(李鹤田, 刘云, 何德全. 信息系统安全风险评估研究综述疆[J]. *中国安全科学学报*, 2006, 16(1): 108-113, 0.)

[14] Feng D G, Zhang Y, Zhang Y Q. Survey of Information Security Risk Assessment[J]. *Journal of China Institute of Communications*, 2004, 25(7): 10-18.
(冯登国, 张阳, 张玉清. 信息安全风险评估综述[J]. *通信学报*, 2004, 25(7): 10-18.)

[15] Zhong Y X. Principles of information science[M]. BEIJING: Beijing University of Posts and Telecommunications Press, 2002.
(钟义信. 信息科学原理[M]. 北京: 北京邮电大学出版社, 2002.)

[16] Zhang H G, Han W B, Lai X J, et al. Survey on Cyberspace Security[J]. *Scientia Sinica* (*Informationis*), 2016, 46(2): 125-164.
(张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述[J]. *中国科学: 信息科学*, 2016, 46(2): 125-164.)

[17] Jiang C Q, Peng Y, Lin J J, et al. CMM$_b$ased Model of Information Systems Security Assurance[J]. *Computer Engineering and Applications*, 2006, 42(34): 112-115, 126.
(江常青, 彭勇, 林家骏, 等. 基于 CMM 的信息系统安全保障模型[J]. *计算机工程与应用*, 2006, 42(34): 112-115, 126.)

[18] Hui Z B, Tang T. Annual Report on Development of Cyberspace Security in China(2015)[M]. BEIJING: Social Sciences Academic Press, 2015.
(惠志斌, 唐涛. 中国网络空间安全发展报告(2015)[M]. 北京: 社会科学文献出版社, 2015.)

[19] Institute of information, Shanghai academy of social sciences. A Dictionary of Information Security[M]. SHANGHAI: Shanghai dictionary publishing house, 2013.
(上海社会科学院信息研究所. 信息安全词典[M]. 上海:上海辞书出版社, 2013.)

[20] Cyber security law of the People's Republic of China, State Council of the PRC, http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm Nov. 2016.

[21] Information technology-Security techniques - Evaluation framework for information systems security assurance (GB/T 20274), National Information Security Standardization Technical Committee, 2008.

[22] National Information Security Standardization Technical Committee, Information security technology - Risk assessment specification for information security (GB/T 20984), 2007.

[23] Xiao G. Current and Future of Information Technology Security Criteria Standards[J]. *Computer Engineering*, 2001, 27(7): 4-6, 13.
(肖刚. 信息技术安全评价标准的现状和发展[J]. *计算机工程*, 2001, 27(7): 4-6, 13.)

[24] US DoD, Trusted Computer System Evaluation Criteria (TCSEC), US DoD 5200.28-STD, 1985.

[25] Office of Official Publications of the European Communities, Information Technology Security Evaluation Criteria (ITSEC) Version 1.2, 1991.

[26] ISO, Information technology - Security techniques - Evaluation criteria for IT security (ISO/IEC 15408-2009), 2009.

[27] National Information Security Standardization Technical Committee, Classified Criteria for Security Protection of Computer Information System (GB 17859-1999), 1999.

[28] Huang Y F. *The Study of Evaluation Criteria for IT Security*[D]. Chengdu: Sichuan University, 2002.
(黄元飞. 信息技术安全性评估准则研究[D]. 成都: 四川大学, 2002.)

[29] Liu W, Zhang Y Q, Feng D G. Survey of Common Criteria Evaluation[J]. *Computer Engineering*, 2006, 32(1): 171-173.
(刘伟, 张玉清, 冯登国. 通用准则评估综述[J]. *计算机工程*, 2006, 32(1): 171-173.)

[30] National Information Security Standardization Technical Committee, Information Technology – Security Techniques – Evaluation Criteria for IT Security (GB/T 18336), 2015.

[31] Wu S Z, Jiang C Q, Lin J J. Information Systems Security Assurance[M]. East China University of Science and Technology Press, 2014.
(吴世忠, 江常青, 林家骏. 信息系统安全保障评估[M]. 华东理工大学出版社, 2014.)

[32] British Standards Institution, Information Security Management. Code of practice for information management systems (BS7799-1), 1995.

[33] British Standards Institution, Information Security Management. Specification of information security management (BS7799-2), 1998.

[34] ISO, Information technology - Security techniques - Code of practice for information security management (ISO/IEC 17799-1), 2005.

[35] ISO, Information technology - Security techniques - Information security management systems – Requirements (ISO/IEC 27001), 2013.

[36] UppercaseISO/IEC 27002: 2007, Information Technology - Security Techniques - Code of Practice for Information Security Management[EB/OL]. 2007.

[37] ISO, Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model (ISO/IEC 21827), 2008.

[38] ISO, Information technology - Guidelines for the management of IT Security (ISO/IEC TR 13335), 1996-2001.

[39] Yang J Z. On the Governance Model of Network Information Contents In Developed Countries[J]. *Jurist*, 2009(4): 130-137, 160.
(杨君佐. 发达国家网络信息内容治理模式[J]. *法学家*, 2009(4): 130-137, 160.)

[40] Measures for the administration of Internet information services, State Council of the PRC, http://www.gov.cn/gongbao/ content/2011/content_1860864.htm? IDTc6TT2Il0, 2000.

[41] Feng J H. The dialectic view of network information security[J]. *Social Sciences Digest*, 2019(3): 5-7.
(冯建华. 网络信息安全的辩证观[J]. *社会科学文摘*, 2019(3): 5-7.)

[42] Regulations on the administration of Internet audio-visual programs, State Administration of Radio, Film and Television, Ministry of information industry, PRC, http://www.nrta.gov.cn/art/2007/ 12/29/ art_1583_26307.html, 2007.

[43] Notice of the state administration of radio, film and television on strengthening the content management of audiovisual programs on the Internet, State Administration of Radio, Film and Television, http://www.sapprft.gov.cn/sapprft/govpublic/10555/333029.shtml, 2009.

[44] Regulations on content management of TV dramas, State Administration of Radio, Film and Television, film and television, http://www.sapprft.gov.cn/sapprft/govpublic/10550/332959.shtml, 2010.

[45] General rules for content review of online audio-visual programs, China Online Audio-visual Program Service Association, http://news.cctv.com/2017/06/30/ARTIm9a7zMhtdUHKCE0OqlfP 170630.shtml, 2017.

[46] Network short video content audit standard details, China Online Audio-visual Program Service Association, http://capital.people.com.cn/n1/2019/0109/c405954-30513159.html, 2019.

[47] Detailed Rules for the Content Audit Standards of Network Variety Shows, China Online Audio-visual Program Service Association, http://www.xinhuanet.com/video/2020-02/21/c_1210484489. htm, 2020.

[48] National Information Security Standardization Technical Committee, Information security technology-Guidelines for the category and classification of Information security incidents (GB/Z 20986), 2007.

[49] Alliance of Industrial Internet, Industrial Internet standard system (v2.0), 2019.

[50] Yang H M, Wang J W. Progress of 5G network security standardization[J]. *Secrecy Science and Technology*, 2019(1): 22-26.
(杨红梅, 王建伟. 5G 网络安全标准化进展[J]. *保密科学技术*, 2019(1): 22-26.)

[51] Feng D G, Xu J, Lan X. Study on 5G Mobile Communication Network Security[J]. *Journal of Software*, 2018, 29(6): 1813-1825.
(冯登国, 徐静, 兰晓. 5G 移动通信网络安全研究[J]. *软件学报*, 2018, 29(6): 1813-1825.)

[52] Notice on Soliciting Opinions on proposal for establishment of national standard project of network security in 2020, National Information Security Standardization Technical Committee, https://www.tc260.org.cn/front/postDetail.html?id=20200611102308, 2020.

[53] Wang C, Zhong Y X. Information Content Security on Internet[J]. *Computer Engineering and Applications*, 2003, 39(30): 153-154.
(王枞, 钟义信. 网络信息内容安全[J]. *计算机工程与应用*, 2003, 39(30): 153-154.)

[54] Cyberspace Administration of China, Regulations on the administration of Internet news and information services, http://www.cac.gov.cn/2017-05/02/c_1120902760.htm, 2017.

[55] Shi W C, Sun Y F. An Analysis of the International Common Criteria for Information Technology Security Evaluation[J]. *Computer Science*, 2001, 28(1): 8-11.
(石文昌, 孙玉芳. 信息安全国际标准 CC 的结构模型分析[J]. *计算机科学*, 2001, 28(1): 8-11.)

[56] Li M. Follow International Dynamics, Find the Gap between Home and Abroad and Promote Technological Development[J]. *Journal of Micrographics*, 2002(2): 25-29.
(李铭. 看国际动态 找国内差距 促技术发展[J]. *缩微技术*, 2002(2): 25-29.)

[57] HORTON F. W. Information resources managemen[M]. LONDON: Prentice Hall, 1985.

[58] Suo C J. Remarks on the Conception and Research Contents of Information Lifecycle[J]. *Library and Information Service*, 2010, 54(13): 5-9.
(索传军. 试论信息生命周期的概念及研究内容[J]. *图书情报工作*, 2010, 54(13): 5-9.)

王宇航 于 2016 年在北京交通大学软件工程专业获得硕士学位, 现在中国科学院大学网络空间安全专业攻读博士学位, 现任中国科学院信息工程研究所助理研究员。研究领域为网络空间安全。研究兴趣包括: 信息内容安全、区块链信息服务安全、机器学习。Email: wangyuhang@iie.ac.cn

郭涛 中国科学院信息工程研究所博士生导师, 研究员, 工学博士。研究领域为网络空间安全。研究兴趣包括: 网络空间安全、漏洞分析与风险评估。Email: guotao@iie.ac.cn

Guo Tao, PhD supervisor in institute of Information Engineering in CAS, Professor, PhD. His main research interests include cyberspace security, vulnerability analysis and risk assessment. Email: guotao@iie.ac.cn

张潇丹 于 2012 年在中国科学院大学计算机系统结构专业获得博士学位, 现任中国科学院信息工程研究所副研究员。研究领域为新型网络技术测量分析与评估。研究兴趣包括: 区块链、互联网数据分析、计算传播等。Email: zhangxiaodan@iie.ac.cn

孟丹 中国科学院信息工程研究所研究员, 博士生导师。研究领域为网络空间安全。研究兴趣包括: 大数据存储与管理, 分布式计算与并行处理, 系统安全理论与技术。Email: mendan@iie.ac.cn

韩冀中 于 2001 年在中国科学院计算技术研究所获得博士学位, 现为中国科学院信息工程研究所正高级工程师, 博士生导师。主要研究领域为大数据存储与管理、多媒体信息智能化处理。研究兴趣: 多媒体内容理解。Email: hanjizhong@iie.ac.cn

周熙 于 2017 年在北京师范大学通信与信息系统专业获得硕士学位, 现为中国科学院信息工程研究所助理研究员, 研究领域为网络安全, 研究兴趣包括: 区块链、网络传播等。Email: zhouxi@iie.ac.cn