国家“十二五”重点规划图书

信息安全管理体系丛书

网络空间安全管理

- 丛书顾问：蔡吉人　周仲义
- 丛书主编：吕述望　赵战生　陈华平
- 执行主编：谢宗晓　吕茂强

谢宗晓　甄杰　董坤祥　主编

林润辉　主审

中国质检出版社

中国标准出版社

网络空间安全管理

谢宗晓　甄　杰　董坤祥◉主编
林润辉◉主审

中国质检出版社
中国标准出版社

北　京

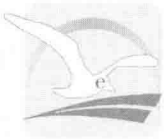
图书在版编目（CIP）数据

网络空间安全管理/谢宗晓等主编. —北京：中国标准出版社，2017.2
ISBN 978-7-5066-8514-6

Ⅰ.①网… Ⅱ.①谢… Ⅲ.①网络安全—安全管理 Ⅳ.①TN915.08

中国版本图书馆 CIP 数据核字（2016）第 305462 号

中国质检出版社
中国标准出版社 出版发行
北京市朝阳区和平里西街甲 2 号（100029）
北京市西城区三里河北街 16 号（100045）
网址：www.spc.net.cn
总编室：（010）68533533 发行中心：（010）51780238
读者服务部：（010）68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 787×1092 1/16 印张 12.25 字数 283 千字
2017 年 2 月第一版 2017 年 2 月第一次印刷
*
定价 39.00 元



国家“十二五”重点规划图书
信息安全管理体系丛书

序言

prologue

中国工程院院士 蔡吉人 推荐序

党中央、国务院高度重视信息安全工作。在中办发〔2006〕11号《2006—2020年国家信息化发展战略》中明确指出："坚持积极防御、综合防范，探索和把握信息化与信息安全的内在规律，主动应对信息安全挑战，实现信息化与信息安全协调发展"，"积极跟踪、研究和掌握国际信息安全领域的先进理论、前沿技术和发展动态"。

虽然信息安全技术和信息安全管理得到了前所未有的重视，但是信息安全事件却一直处于有增无减的状态。只有信息安全技术和管理并重，在宏观层次上实施了良好的信息安全管理，才能使微观层次上的安全，如物理措施等，实现其恰当的作用。采用信息安全管理体系并得到认证无疑是组织应该考虑的方案之一。事实上，也只有这样才能真正站在组织的高度上来对待信息安全问题。

信息安全管理体系（ISMS）是基于组织业务风险方法来建立、实施、运行、监视、评审、保持和改进信息安全，它跳出了"为安全信息而信息安全"的传统概念，强调站在组织业务的角度来管理信息安全活动。ISMS相关标准不仅为一个组织提供从框架到细节的全面指导，而且为ISMS的整个产业链提供指南。

基于此，中国质检出版社组织了国内的信息安全专家及标准的起草者编写了《信息安全管理体系丛书》。本丛书是我国第一套全面系统的信息安全管理体系丛书，它从ISMS的基础信息安全风险管理开始讨论，从

不同领域、多个侧面，对ISMS相关知识进行了细致的介绍和阐述，有理论，更有实践，包括ISMS的审核指南、应用方法、业务连续性管理以及在重点行业的应用实例，很有特色，可谓既专又广，是一套充分展示ISMS领域当前成果并将其推广的优秀图书，一定会为我国ISMS专业人才的培养起到重要的推动作用。

2012年9月

序言

prologue

中国工程院院士 周仲义 推荐序

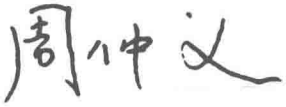
当前，国际上围绕信息的获取、分析、利用和控制的竞争越来越激烈，信息安全已成为维护国家安全、保持社会稳定、关系长远利益的关键组成部分，备受各国政府的关注和重视。如何确保信息安全已是各国政府及各种组织改进其竞争能力的一个新的具有挑战性的任务。

入选国家“十二五”重点图书规划的出版项目《信息安全管理体系丛书》，融入了作者多年来在信息安全、信息安全管理体系领域的研究和实践成果，包括多项具有自主知识产权的创新成果，是面向现代信息安全从业人员普及国家信息安全政策和信息安全知识，强化组织信息安全意识和信息安全保障能力建设，展示信息安全领域最新成果和信息安全管理体系建设、实施、运行、审核成就的高水平通俗读物。

该套丛书共有13个分册，主要内容涉及信息安全风险管理和风险评估、信息安全管理体系实施、信息安全管理体系审核、业务连续性管理、信息安全管理体系与ISO/IEC 20000的整合、信息安全管理体系与信息系统安全等级保护的整合以及信息安全管理体系在重点行业和领域的应用。书中各种典型的案例，针对各种网络安全问题的应对措施，为组织提供了一个完整的业务不间断计划，能为组织业务的正常运行起到保驾护航的作用。

该套丛书主要作者长期从事信息安全领域的科学研究与实践，曾参

与多项信息安全国家标准的制修订，经验丰富，成果丰硕。他们编著的这套《信息安全管理体系丛书》，可代表现阶段我国信息安全管理体系领域最高研究水平，在服务于国家或组织，提升国家安全战略方面将起到非常重要的作用，必将产生显著的社会效益。该套丛书的出版，在我国工程技术领域是具有重要意义的大事，将为我国信息安全保障能力建设提供有力的支撑，让信息安全管理体系真正成为对抗信息霸权主义、抵御信息侵略的重要保障。



2012 年 9 月

丛书前言

Series introduction

信息通信技术（ICT）的快速发展和广泛应用，为人类开拓出继陆、海、空、天之外的第五维生存空间——赛博空间（Cyberspace）。ICT 的潜能不但使赛博空间展现出前所未有的美好前景，也为人类在陆、海、空、天的生产活动、科学研究以及知识学习、文化传承与交流和社会管理带来了高效率、高效益。信息化成为当今社会发展的巨大推动力。

但是，在新技术的应用中，风险和机遇并存。技术的不成熟，使得社会犯罪分子利用这些技术的漏洞谋取利益；霸权国家为其核心利益展现的把赛博空间作为新的战争空间的国策，使赛博空间显现出不和谐、不安宁的不良态势。

探究当代各国的信息安全战略和实践可知，提升信息安全保障能力是应对危机的对策，技术与管理并重是保障能力提升的出路，风险管理是指导保障能力形成的思想。

保障能力体现于预警能力、保护能力、检测能力、响应能力、恢复能力和反制能力。

技管并重要求，信息安全保障能力建设不但需要运用技术手段，还要运用管理手段，并且要运用技术手段支持管理手段，运用管理手段提升技术手段应有作用的有效发挥。

风险管理的思想使我们清醒地认识到，面对信息系统的应用，我们实际上是面对一个人机结合的、智能化的、非线性的时变复杂大系统。我们所做的防护努力，只能减少信息安全事件发生的可能性和发生事件

的损失及影响。绝对杜绝事件的发生是不可能的，我们必须积极应对处置可能发生的事件，保障依赖信息系统要完成的使命。

信息安全已经从关注技术平台发展到关注业务使命和组织治理。信息安全保障也提升到了依赖信息化手段的使命保障。我们需要跟上这个提升，研究思考和部署更高层次的安全保障。

信息安全管理的理论和实践，已经从依据长官意志的人治型管理，经由制度化建设的规章型管理，发展到了根据管理理论和成功实践经验加以规范化、标准化的体系化管理。ISO/IEC SC 27 的 27000 系列标准将不断丰富和完善的信息安全管理体系（ISMS）展现在我们面前。发达国家结合国情，也各自拥有与 27000 系列指导思想相一致的相关标准（例如美国国家标准与技术研究院开发颁布的风险管理框架 NIST 特别出版物 SP 800的相关系列标准）。我国信息安全标准化技术委员会已经把 27000 系列定为国家标准，同时结合国情颁布了若干为等级保护所需要的信息安全管理标准和风险评估、风险管理、事件分级分类、处置、灾难备份恢复等国家标准。

本系列丛书的目的在于跟踪国际和国家标准的发展，分析解析标准的内涵要义，试图帮助读者加深理解标准，也试图以总结作者的实践案例来宣贯标准，帮助读者正确地实施标准，执行标准。

信息安全保障能力是信息化条件下的综合国力的体现，能力低下必定吃亏挨打。我们不能满足我国信息化的发展速度和规模。我们必须依靠自己和世界上平等待我的朋友一起共建赛博家园，保障赛博家园的安康。

中国科学院信息安全国家重点实验室

2012 年 8 月

丛书主编吕述望教授的话

在 Internet 上搞中国的信息安全是不可控的，事实上，对于 Internet 而言，美国以外的国家都只是安全利用的问题。为什么这么说呢？这要从以下几点说起。

1. 互联网定义：互联网是两个以上的具有一个主根的网络的平等连接。其上层不再有根。

2. Internet 网是人类的重要建树，其中文译名为因特网。它是美国的国际网，可记作 USA-i-Net 。

3. 中国公众使用的网络实际上也是 USA-i-Net，中国用户域名 .cn。我们使用 IP 地址是要给美国人付钱的，而且，.cn 受 Internet 主根的控制，毫无安全保证。

4. 目前中国网络语言“互联网”指的是美国的国际网。“中国是互联网大国”指的是“Internet（因特网）用户大国”，“中国互联网协会”指的是“Internet 中国用户协会”。

5. 党和国家的领导人已经认识到了这一问题的严重性。2010 年 6 月 7 日，胡锦涛总书记在中国科学院、中国工程院两院院士大会上发表了“要积极研发和建设新一代互联网”，“改变核心技术受制于人”的讲话。“新一代互联网”的概念显然不是对现在 Internet 的改造，因为从前面的讲述可知，在 Internet 上实现中国的信息安全无异于缘木求鱼。

6. 中国应该建设中国国际网（CHINA-i-Net）。中国国际网的协议如

果与美国国际网（Internet）一致也可，使用 IPv9 可能容量会大，权利纷争会小。问题的关键是中国有了主根，且有了与国际平等连接的物质基础与思想准备。

7. CHINA-i-Net，USA-i-Net 等多个网络平等连接，自然形成互联网，世界未来网络是不会依附任何一个国家的。未来网络中的认证，识别，安全保密会有全新的概念与技术出现。数字世界是由数字序列、知识包、知识阅读器三部分组成的，人类将在数字世界里平等、自由、负责地畅游知识的海洋！

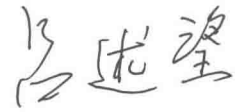
8. 有关互联网的项目要立足中国国际网（CHINA-i-Net）。我国北斗卫星导航系统与美国全球定位系统 GPS 是个好例子。

9. 除了加强 Internet 的安全利用，全面的信息安全管理也非常重要。

为此我们组织编写了《信息安全管理体系丛书》，并有幸被列入了国家“十二五”重点图书规划，这也表明了国家对信息安全问题的高度重视。

我深切期望，《信息安全管理体系丛书》的出版能为 Internet 的安全利用，为国内信息安全管理现状的提升尽绵薄之力。

中国科学院信息安全国家重点实验室
北京知识安全工程中心



2012 年 8 月

序 言

prologue

从信息安全到网络空间安全

信息安全的三层内涵

从通信安全、计算机安全到网络安全（network security）、互联网安全，以及今天的网络空间安全（cyberspace security）[1]，信息安全越来越成为国家、社会、企业、个体关注的核心问题。这是因为安全是社会发展的前提，从系统论和信息论角度看，信息安全是一切安全的基础，而信息传输信道、信息处理设备、信息互联架构和信息存在空间的安全目的都仍是从各个角度保证信息的安全。

我们在《信息安全：从 4A 到 4R》[2] 的文章中谈到，信息安全有三个层次：信息（自身）的安全；信息系统的安全；信息安全和信息系统安全引致的传统（生命、财产、物质、社会、心理）安全。信息技术和网络技术改变了人的思考方式和行为模式，改变了安全管理中技术与管理的角色。提高信息安全需要打造信息安全研究与实践的知识价值链。

第一个层次——今天，信息化和全球化时代，信息成为组织的战略性资源，信息安全更加重要。尤其是对于那些信息密集型组织，如轻资产公司，信息成为其战略资源，信息安全成为组织生存、发展、创新之根本；和黄金、石油类似，信息也成为一个国家运行发展、长治久安的核心资源；所以，在物联网、互联网和社会网络互动的时代，即时产生海量信息，信息质量需要鉴别，过载信息、虚假信息、无关信息、过时信息无处不在，这些信息自身就有安全问题。

第二个层次——信息系统是信息采集、加工、存储、组织、管理、传播的工具，是信息处理的硬件、软件、网络支撑体系的集合。信息系统的安全直接导致信息的安全。今天上述过程已经全面构建在网络结构、全球互联为架构的信息基础上设施之上，信息系统的

---

〔1〕 此处不赘述相关词汇的区别，请参考本书正文中的论述。

〔2〕 4A（Anytime Anywhere Any type of information to Anybody），4R（Right information to Right people at Right time in Right place）。

全文见：林润辉，谢宗晓．信息安全：从 4A 到 4R［J］．中国标准导报，2015，05：26－29.

安全，也全面升级为互联网、物联网、云服务等网络基础设施系统（包括软件和硬件）的安全。

第三个层次——信息自身安全、信息系统安全引致的传统安全。表现为生命、财产安全，行业关联的生产安全、交通安全、金融安全，乃至国家、社会安全等。

以上信息安全的三个层次相互关联、相互影响，形成了信息安全管理的核心和分析基础。

信息安全的三重空间

和自然空间和社会空间对应的是网络空间。网络空间（cyberspace）是一个由机器、用户及其关系所组成的虚拟世界，这是一个建立在信息技术基础之上的完整空间，这意味着人们生活在一个由自然、社会和（网络）虚拟空间构成的世界之中[3]。

其中自然空间是人类作为生物体的存在之本，自然空间造就了人类，尽管人类试图影响环境、改造自然。社会空间与人类共同演进，包括自然组成部分的人类自身（自然人和社会人）及其塑造的社会－技术系统；网络空间是人造空间，包括1）所有的网络信息技术设施；2）自然空间、社会空间对应的数字化、虚拟化的映射（包括数字化的自然空间，各种反映自然的数字化要素，如Google Earth，Google Ocean，数字月球等），数字化的社会空间，包括数字化的人、数字资产、数字化的组织等，如典型的虚拟空间第二人生（The second life）；3）其他所有数字化的数据、信息、知识等。

所以，信息技术革命以来人类创造的一切数字化的对象、内容以及信息网络设备、系统、技术设施都是网络空间的内容，它们也构造了网络空间。网络空间包括了数字化的信息，网络信息系统、网络信息设备、网络信息基础设施以及数字化的自然空间和社会空间。

信息安全存在并作用于自然空间、社会空间和网络空间三重空间中。信息自身的安全存在于所有三重空间中，信息系统安全存在于社会空间和网络空间二重空间中，网络空间安全包括网络空间中的信息自身安全、网络信息系统和网络基础设施安全，以及虚拟自然空间、虚拟社会空间的结构和运行安全。网络空间安全的引致安全会从网络空间扩散到社会空间以及自然空间。

网络攻击、无人机的应用，使得网络战、信息战成为新升级的战争模式，致使信息自身的安全直接影响生命、财产安全，乃至国防安全；地震预报信息、谣言等直接影响民众情绪和公共秩序与安全；信息系统深度嵌入业务系统，金融信息系统不安全，会导致银行系统崩溃，引致财产安全和社会混乱；交通信息系统故障，会导致交通事故，引致生命、财产安全；电网信息系统问题，会形成能源事故，引致社会运行瘫痪。所以网络空间中存在安全问题，网络安全的引致安全也会渗透到社会空间中。

〔3〕 张康之，向玉琼．网络空间中的政策问题建构．中国社会科学，2015，02：123－138＋205.

同时信息安全引致的核电事故、核威胁、核打击后果，排放事故、化石能源控制不利等也会带来环境污染、生态破坏。相反基于系统控制的滴灌技术、系统，分布式能源系统，以及新能源和自动驾驶技术和系统会有效减少和缓解自然空间中的环境和生态风险。

网络空间安全问题会通过信息安全、信息系统安全扩散到社会空间、自然空间中。

网络空间安全与管理

网络空间安全包括四个方面：一是网络空间中一切数字化信息自身的安全（网络空间中信息自身安全：包括网络空间中的信息内容；数字化的自然空间和社会空间，即以数字化形式存在的自然和社会映射），二是网络信息系统和网络基础设施安全（网络空间信息系统安全（硬件（实体）、软件和服务）），三是网络空间中数字化社会、数字化自然的运行安全，以及上述网络空间安全问题的引致安全，引致安全存在于社会空间和自然空间中。

三重空间的信息安全是相互联系和互动的，网络空间安全会导致社会空间和自然空间的引致安全，同时自然空间的问题如地震、太阳辐射等也会引发网络信息系统安全，影响网络空间安全；社会空间中的安全问题，如人为破坏、黑客攻击、超负荷访问也会影响网络空间运行，导致网络空间安全和网络空间信息安全问题。

网络空间安全的层次

如同社会（空间）安全管理一样，也可以从个体、组织和国家、国际组织等层面分析网络空间及网络空间安全问题。

网络空间安全个体层次分析：隐私属于个体信息安全内容，一旦个人隐私信息数字化，隐私信息便同时存在与社会空间和网络空间中，网络空间管理有效，有助于数字化隐私信息的保护。如果保护不利，网络空间个体层面信息安全风险随之提高，这类问题多数由于社会空间和网络空间接口问题（制度、管理手段等）形成，这会增加个人信息安全的风险；

组织层面的网络空间安全：组织包括企业组织、非营利组织和政府组织，体现在社会空间中各类组织运行需要网络空间支撑，组织越来越多的数字资产、资源存在于其对应的网络空间中，组织在相互渗透的社会空间和网络空间中存在，组织也有了社会空间和网络空间的边界。同时，不同组织的网络空间相互渗透和结合，组织需要定义自身网络空间边界，明确与其他组织的网络空间接口和在上一层次网络空间嵌入的协议和标准，实现社会空间中实体组织和网络空间中虚拟组织（组织在网络空间映射和投影）的联动；推动企业电子商务、组织电子服务、政府电子政务的深化，推动 O2O 的深化；同时关注组织社会空间信息安全和网络空间信息安全，方能实现真正的信息安全；

国家层面的网络空间安全：国家主权决定了网络主权，需要定义国家网络空间的主权边界，但国家地理边界和网络主权边界相互联系又不完全相同，比如基于国家安全考虑将一些数据服务器位于国境内的要求成为基于社会空间和地理边界确定网络空间权力边界的

操作方式，此时两种边界统一；同时一个国家的跨国公司、使领馆、海外组织使得信息、数据、设备等网络空间边界突破国家边界，在全球网络空间中形成一个多维、立体、弹性、边界模糊、时变的空间结构子网。所以国家层面的网络空间安全，要强调网络主权，同时要直面网络空间边界确定的难度和根据具体安全问题进行界定和管理的原则。

网络空间安全管理的对策

网络空间安全管理的内容包括网络空间中的信息内容管理，即信息自身安全（数据，信息，知识库，专利，程序）；网络信息系统安全（操作系统，软件系统安全，硬件网络基础设施安全，云安全）；以及网络空间运行的制度体系安全和源自网络空间影响的社会空间、自然空间的引致安全。

信息安全的多层次内涵、网络空间安全多层次结构，以及三重空间的嵌套和渗透，使得网络空间安全重要而复杂。

国际上，网络空间安全问题日益突出。习近平指出："从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透……""……必须维护网络空间安全以及网络数据的完整性、安全性、可靠性，提高维护网络空间安全能力"。

随着信息数字化程度深化，自然空间，尤其社会空间运行的数字化程度加深，对于网络基础设施依赖程度日益提高，网络空间安全成为信息安全问题的核心和关键。网络空间的安全管理，呈现了如下特征：

一是网络空间中技术基础设施结构网络化。互联网、万维网呈现无标度网络结构，定点攻击尽显脆弱性，结构特征决定网络空间安全风险更具系统性，信息安全问题具有跨空间传染性，这都增加了网络空间安全问题的风险。

二是网络空间中信息内容本身全部数字化，传播速度快，一旦有漏洞，瞬间可能形成巨大损失；而数据开放又是共享和创新的前提，这使得网络空间信息安全管理挑战增加，难度提高。

三是各个国家、各类组织网络空间边界模糊，界定困难。三重空间界面交织，国家、组织的网络空间相互渗透，既要界定边界，维护网络空间主权和权利，实现安全的"分离"，又要顺应趋势，定义"连接"，促进信息共享和价值共创。所以，针对网络空间安全问题，定义可以管理的界面（manageable interface）变得至关重要。

四是网络空间安全问题跨空间联动，时变性强，复杂性高。网络空间安全问题既可以在不同层次上转化、延伸，也在三种空间之间渗透、扩散、放大，导致网络空间安全风险来源更加多样化，传导、扩散路径多样化，安全后果更加严重和具有外部性。

基于上述特征，网络空间安全管理需要新的策略：

首先是多点监测、立体监控。通过技术和管理手段，对于网络空间内容模块、系统模块和界面模块进行多点监测，立体监控，随时发现信息安全隐患、异动，实时预警，即时

处理；

其次是实施网络空间安全分类、分层管理。基于信息安全管理价值链界定安全问题属性；从信息安全内涵不同层面，网络空间主体的不同层面，对于网络空间安全问题进行针对性的分层管理；区分技术和管理角度，区分网络空间安全问题来源，区别网络空间安全管理主体，区分网络空间安全问题对象，区分技术设施不同网络拓扑结构，区分信息安全风险扩散机理，分类制定和采取不同的管理措施；

然后是围绕网络空间安全问题实施共同治理。网络空间安全涉及社会空间众多的利益相关者，包括各国各级政府、企业、用户、非营利组织、大学等技术供应组织、网民等，不同层面网络空间相互渗透、嵌套和集成，网络空间安全需要共同的意识、协调的规则以及兼容的标准，需要一个网络空间安全治理的对话、研究、规则制定和实施平台，这是网络空间安全保障的制度基础。

最近我参加了一项国际合作项目，来自中、美、德、日、印五国的研究者针对互联网治理进行研究，出版了 Shared responsibility，toward more inclusive internet governance 的报告[4]。核心思想是互联网这样一个全球公共物品，需要不同国家各类利益相关者的共同参与和协同治理，方可实现互联网的创新发展、包容发展和可持续发展。同样在第二届世界互联网大会上，习近平主席提出了全球互联网发展治理的“四项原则”和“五点主张”。推动互联网全球治理体系变革，实施全球网络空间安全合作，打造安全的网络空间，是实现网络空间命运共同体目标的必由之路。

林润辉

2016 年 12 月 2 日于南开大学商学院

[4] http://www.bosch-stiftung.de/content/language2/downloads/GGF2025_Internet_Governance_RZ_Web.pdf