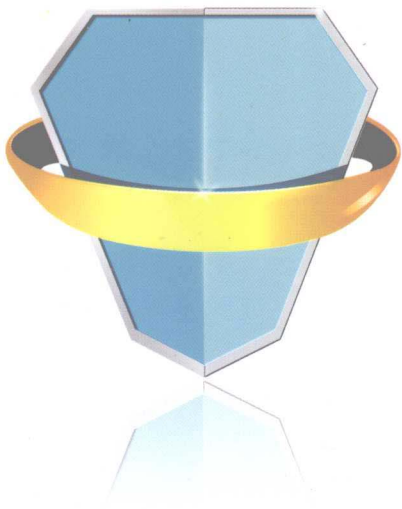
INDIVIDUAL INFORMATION SECURITY

个人信息安全

—研究与实践

STUDY AND PRACTICE

郎庆斌 孙毅 ◎ 著



人民出版社

个人信息安全

——研究与实践

INDIVIDUAL
INFORMATION
SECURITY
STUDY AND
PRACTICE

人民出版社

责任编辑:高晓璐
装帧设计:艺和天下

图书在版编目(CIP)数据

个人信息安全——研究与实践/郎庆斌　孙　毅　著.
　-北京:人民出版社,2012.11
ISBN 978-7-01-011344-9

Ⅰ.①个…　Ⅱ.①郎…②孙…　Ⅲ.①计算机网络-隐私权-安全技术　Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2012)第 246656 号

个人信息安全
GEREN XINXI ANQUAN
——研究与实践

郎庆斌　孙　毅　著

人民出版社 出版发行
(100706　北京市东城区隆福寺街 99 号)

北京新魏印刷厂印刷　新华书店经销

2012 年 11 月第 1 版　2012 年 11 月北京第 1 次印刷
开本:710 毫米×1000 毫米 1/16　印张:16.5
字数:260 千字

ISBN 978-7-01-011344-9　定价:39.00 元

邮购地址 100706　北京市东城区隆福寺街 99 号
人民东方图书销售中心　电话 (010)65250042　65289539

◎前　言◎

本书是继《个人信息保护概论》、《个人信息安全》后的第三本有关个人信息安全专著，它既是《个人信息保护概论》的先导，也是对近十年参与个人信息安全标准体系建设的理论研究和力行实践验证的总结。

本书试图构建个人信息生态系统的基本框架，并尝试基于个人信息生态系统研究个人信息安全的深层原因。在个人信息安全领域中，个人信息保护是研究与手段相关的法律适用、技术适用、管理适用、标准适用等的策略和方式方法。个人信息安全则应是以个人信息的生态环境为基本框架，综合、统一、系统、科学、完整地研究个人信息复杂生态系统的相互关联、相互作用和相互影响，及与个人信息生态相关的社会生态、社会形态、环境因素、技术进步、安全失衡等的安全策略、安全管理、安全机制等。

个人信息安全是随着社会进步、科技发展，特别是信息技术的发展，从信息安全领域衍生出的新的分支、新的研究领域。实现个人信息安全，需要基于个人信息生态系统，以有效、能动、可控、安全为目的，约束、规范针对个人信息及相关资源、环境、管理体系等的相关管理活动或行为，提高服务管理能力和服务管理质量。

本书在撰写中，修正了前两本著作中的一些概念、观点和实践验证中的问题，提出了个人信息生态系统和其他一些新的概念、思想，借以与个人信息安全研究者共同研究和探讨，以期探索符合中国国情的个人信息安全模式、理论基础和实践验证手段。

全书由郎庆斌撰稿，第六章、2.2节、4.1节、5.4节及附录部分由孙毅编写和组织。本书在编写过程中，中国社会科学院法学研究所吕艳滨先生审阅了部分章节，提供了有益的思路；也得到许多关注个人信息安全人士的大力支持和帮助，谨借此表示衷心的感谢。

大连交通大学

郎庆斌

2012年6月18日

目录

centents

第一章
绪 论

信息与能源、材料并称现代文明的三大支柱，能源、材料是人类生存和社会发展的基本资源；信息则是区别于能源、材料的较为高级的、独立的资源，为人类提供知识和智慧。

信息是人类对客观存在的事物的反映，是对自然、社会的现象、本质、特征、规律的描述。信息的内涵和外延很宽泛，大到政治、军事、经济等，小到商业、企业、个人等，是人类生产活动、社会活动中的基本载体，承载以文字、符号、声音、图形、图像等形式，通过各种渠道传播的信号、消息、情报、资料、文档等内容。如近年来的禽流感、毒奶粉、汶川大地震、甲型H1N1流感等。

信息安全，顾名思义是保证信息的安全。信息安全是随着社会进步、科技发展，特别是信息技术的发展不断扩展、延伸和深化的。广义角度，信息安全是保证自然、社会相关信息的状态、信息所依附的管理、技术及安全体系免受威胁、侵害；狭义角度，各类组织的信息资源不因偶然的或故意的因素，非法或未授权泄露、更改、破坏，及信息内容不被非法控制、识别、篡改。

本书所涉及的信息安全，是IT安全和个人信息安全。

1.1 IT的概念

IT（Information Technology），信息技术，是信息化过程中，与信息产生、发送、传输、接受、处理、存储、交换、识别、控制等相关的应用技术。

信息技术，一般包括3个层次：

a．基础设备。支撑信息化的基础设备，包括网络设备、处理和传输设备、数据存储设备、安全设备、计算机终端等等及相关技术；

b．应用平台。承载信息化应用的软件系统，包括系统平台（windows、Unix等）、支撑软件（数据库系统、接口软件、工具软件等）、安全系统（病毒防护等）等等及相关技术；

c．应用系统。利用基础设备、应用平台解决各种实际问题的应用软件。包括科学计算、数据处理、知识获取、事物处理、辅助设计、业务管理等等及相关开发技术。

随着IT行业的分化、融合、发展、成熟，IT的语境（context）逐渐发生变化，由狭义逐渐延伸、扩展到广义。缩略语“IT”，已经不能简单地翻译为“信息技术”。如“IT标准”、“IT服务”、“IT运维”等，不能简单地翻译为“信息技术标准”、“信息技术服务”、“信息技术运维”。

“IT”语境所涵盖的，应该包括：

a. 信息资源：

信息资源是各类组织逐步累积的信息、信息系统、生产、服务、人员、信誉等有价值的资产，是由人、信息和信息技术三元素构成的有机整体，是信息化的基本要素。根据信息资源的属性、特征，主要包括6类：

1．信息资产：各类组织运营、服务涉及的数据、信息等；包括科技资产（技术、专利、机密、创新等）、生产资产（运营、服务中形成的各种信息，包括各类数据库、相应文件、合同和协议、文档、成本相关的各种信息等）、市场资产（组织运营、服务的外部相关信息）、宏观资产（组织生产、发展的宏观环境信息）及管理资产（信息资产的管理）；

2．软件资产：支撑信息资产生成、处理、分布、存储、检索、传输、交换、管理等的各类软件系统，如系统软件、应用软件、支撑软件、开发工具、服务等及相应的技术资产（软件系统的管理、应用、维护、支持等）；

3．硬件资产：保障信息资产、软件资产安全、稳定、可靠运行的基础设施，如计算机设备、网络设备、通信设备、移动介质及其他相关设备等及相应的技术资产（硬件基础设施的管理、应用、维护、支持等）；

4．物理资产：保障组织运营、服务的工作环境安全的物理设施，如门禁、监控等及相应的技术资产（物理设施的管理、应用、维护、支持等）；

5．人员资产："人"是信息资源的核心，利用智力和信息技术，控制信息资源，协调相关的活动和行为。因而，人员资产是重要的信息资源，涵盖组织的各类员工以及人力资源管理；

6．无形资产：没有实体形态、具有潜在利益的信息资源，如商标、信誉等，也包括员工个人的姓名、荣誉、名誉、肖像等及相应的管理资产（无形资产的管理）；

b．信息技术：

包括前述的3个层次。

c．信息服务：

根据服务环境特征、服务内容特征，采用信息技术，基于信息资源提供的多种服务，主要由服务策略与方法、服务对象、服务周期和服务内容四个要素构成。其中，服务周期包括服务支持、服务提供和服务交付3个阶段。

信息服务可以分为3大类：信息传输服务、IT服务和信息资源服务（包括产业）。主要包括：系统集成、软件工程、服务外包（ITO、BPO、KPO等）、数据库、系统运维、增值业务、内容管理、电子印刷、信息产业及提供专业服务的专门公司等等。

信息服务的特点是以用户需求为导向，以质量管理为核心，以中间产品服务为形式，提供多样化的生产关系、市场化的经营方式和规范化的服

务管理。

d. 服务过程：

采用信息技术，基于信息资源提供的服务，由服务过程形成产品，体现了人、信息、信息技术之间的关联，是服务周期、服务对象和服务组织之间行为和活动的整合管理。

e. 服务质量：

在采用信息技术，基于信息资源提供服务的过程中，实施全面质量管理，保证服务产品的可用性。

因而，“IT”已不仅仅是信息技术的缩写，表达的是一个宽泛的概念。

IT安全，是基于信息技术，以信息资源为核心，提供安全的信息服务管理环境。

1.2 信息安全简述

信息安全是一门涉及各种安全理论、技术和管理的综合性学科，包括计算机科学、计算机网络技术、通信技术、信息安全技术、信息资源管理技术、物理环境安全技术等，以及应用数学、信息论、管理科学等多个学科。

信息安全的基本目标包括：

a. 保密性：保证信息在存储、使用、处理、传输、交换过程中不会泄露，或无法理解真实含义；

b. 完整性：保证信息在存储、使用、处理、传输、交换过程中不被篡改，保持信息的一致性；

c. 可用性：保证授权用户合理、可靠、实时使用信息资源，不被异常拒绝；

d. 真实性：判断、鉴别信息来源的真实、可靠；

e. 不可抵赖性：保证信源与信宿对其行为的责任和诚实。

信息安全具有5个特性：

a. 信息安全的全面性。

根据传统的木桶理论，木桶是由许多块长短不同的木板制作的，木桶容水量大小取决于其中最短的那块木板，而不是其中最长的那块木板或全部木板长度的平均值。因此，提高木桶整体效应的关键在最短的那块木板的长度。

根据这一理论，在信息安全中，信息安全程度取决于系统中最薄弱的环节。但同时应看到，木桶是一个整体结构，其桶底的承载力、桶箍的耐受力和其他木板的合力，构成了木桶的整体效应。因此，桶底的承载力即是信息安全的基础，而桶箍的耐受力和其他木板的合力构成了信息安全的关键。在改善信息安全薄弱环节的同时，应在风险评估的基础上，构建信息安全整体框架，坚固信息安全的基础，加强信息安全的关键。

b. 信息安全的过程性和完整性

信息安全是一个动态的复杂过程，贯穿于信息资源和信息系统的整个生命周期。这个生命周期包括一个完整的安全过程，这个过程包括：系统的安全目标与原则的确定、系统安全的需求分析、系统安全策略研究、系统安全标准的制定、风险分析和评估、系统安全体系结构的研究、安全工程实施范围的确定、安全方案的整体设计、安全技术与产品的测试与选型、安全工程的实施、安全工程实施的监理、安全工程的测试与运行、安全教育与技术培训、应急响应等。

c. 信息安全的动态性

随着信息技术的不断发展，潜在的安全威胁越来越大，攻击和病毒的出现，越来越频繁，越来越花样百出。因此，安全策略、安全体系、安全技术也必须动态调整，使安全系统不断更新、完善、发展，能够在最大程度上发挥效用。

d. 信息安全的多层次立体防护

信息系统的威胁是始终存在的，应用和实施基于多层次立体防护安全系统的全面信息安全策略，采用多层次的安全技术、方法和手段，增加攻击者侵入所花费的时间、成本和所需要的资源，可以有效地降低被攻击的危险，达到安全防护的目标。

e. 信息安全的相对性

信息安全是相对的，没有100%的安全。所有安全问题必须与相应的风险、成本和效益进行定性、定量分析。信息安全的多层次防护就是基于这一共识制定的策略、方案和承诺。

1.3 个人信息安全简述

广义的信息安全是保证自然、社会相关信息的状态、信息所依附的管理、技术及安全体系免受威胁、侵害。个人信息安全是随着社会进步、科技发展，特别是信息技术的发展，衍生出的新的分支、新的研究领域。

信息安全是介于自然科学、系统科学、数学与社会科学、哲学之间的新兴的交叉学科，根据其研究内容、理论和实践的特征差异，个人信息安全是一个重要的研究领域。

在个人信息安全研究中，涉及个人信息的形态、特征、系统演化、社会学意义，以及安全机制、安全技术、管理科学、安全评价等多个方向。

个人信息安全的基本目标，包括：

a. 完整性：保证个人信息在收集、存储、管理、处理、使用、传输、交换等过程中，不被破坏、损毁。完整性包括：

1. 识别因子的完整性。在个人信息中，可识别个人信息主体的关键因素，可以称为识别因子。个人信息主体是可识别的，其识别因子是唯一的；

2. 参照元素的完整性。在个人信息中，识别因子之外的组成元素，可以称之为参照元素。参照元素可间接识别个人信息主体，也必须是完整的。

b. 准确性：保证个人信息在收集、存储、管理、处理、使用、传输、交换等过程中，不被篡改，可以准确识别、描述个人信息主体。准确性包括：

1. 过程保证。个人信息收集、存储、管理、处理、使用、传输、交换等过程，必须保证完善的质量管理，保证其科学性；

2．方法合理。个人信息收集、存储、管理、处理、使用、传输、交换等，必须保证其方法合理、有效；

3．来源可靠。必须保证个人信息来源真实、可靠。不能收集、存储、管理、处理、使用、传输、交换琐碎的个人信息。

c．时效性：

1．必须确定个人信息的保存期限；

2．必须适时更新，保持个人信息的最新状态。

d．不可抵赖性：保证个人信息管理相关行为的责任和诚实。

个人信息安全具有与信息安全类同的特性：

a．全面性：在风险评估基础上，构架个人信息安全整体架构，全面、全方位建设个人信息安全管理体系；

b．过程性：个人信息安全，体现在复杂的过程中。过程是依靠个人信息安全管理体系实现；

c．动态性；随着社会进步、科技发展，特别是信息技术的发展，安全风险、安全威胁在动态变化，个人信息安全管理体系必须动态调整，适时改进、完善；

d．多层次立体防护：个人信息安全的过程性和动态性，要求从管理、业务、环境、技术等多方面、深层次构建个人信息安全管理体系；

e．相对性：个人信息安全同样是相对的，没有100%的安全。

IT安全与个人信息安全是信息安全的两个分支，二者互为融合，互为依托。区别个人信息安全与IT安全的关键，在于：

a．个人信息安全是基于保证个人信息、个人信息主体权益的安全；

b．IT安全是基于信息资源安全展开的。

1.4 个人信息生命周期

生命周期是一个生命体从出生到成熟再到衰退的过程。生命周期理论运用于自然、生态、系统、管理、技术、人等，反映出生命周期各个不同