互联网可信生态环境研究

刘月琴 康艳梅 李顺◎编著

知识产权出版社
全国百佳图书出版单位

本书出版由国际关系学院中央高校基本科研业务费专项资金资助

互联网可信生态环境研究

刘月琴 康艳梅 李顺◎编著

知识产权出版社
全国百佳图书出版单位

图书在版编目（CIP）数据

互联网可信生态环境研究/刘月琴，康艳梅，李顺编著. —北京：知识产权出版社，2017.9

ISBN 978-7-5130-4909-2

Ⅰ.①互… Ⅱ.①刘…②康…③李… Ⅲ.①互联网络—生态环境—研究 Ⅳ.①TP393.4

中国版本图书馆 CIP 数据核字（2017）第 111956 号

内容提要

当前在互联网建设领域领先的国家，已将注意力聚焦在如何保证网络行为的安全性，网络身份的真实性，建立基于身份识别系统的网络可信生态环境。本书在系统调研美国等发达国家互联网可信生态环境的基础上，着重分析了我国互联网可信生态环境现状，提出了建设我国互联网生态环境的对策建议。

责任编辑：蔡　虹　　**责任出版：**刘译文

封面设计：邵建文

互联网可信生态环境研究

刘月琴　康艳梅　李　顺　编著

出版发行：知识产权出版社有限责任公司	**网　　址：**http://www.ipph.cn
社　　址：北京市海淀区气象路 50 号院	**邮　　编：**100081
责编电话：010-82000860 转 8324	**责编邮箱：**caihong@cnipr.com
发行电话：010-82000860 转 8101/8102	**发行传真：**010-82000893/82005070/82000270
印　　刷：北京嘉恒彩色印刷有限责任公司	**经　　销：**各大网上书店、新华书店及相关专业书店
开　　本：787mm×1092mm　1/16	**印　　张：**14.25
版　　次：2017 年 9 月第 1 版	**印　　次：**2017 年 9 月第 1 次印刷
字　　数：200 千字	**定　　价：**45.00 元

ISBN 978-7-5130-4909-2

互联网可信生态环境建设已成为国家战略

当前，世界互联网发展正在进行重心偏移，由“基础设施建设”到“应用系统建设”再到“可信生态建设”，建立基于身份识别的互联网可信生态环境已经成为各国网络发展战略的重要目标。

互联网可信生态环境概念最早由美国提出。2011年4月15日美国白宫公布《可信互联网空间身份标识国家战略》(《National Strategy for Trusted Identities in Cyberspace》，简称“NSTIC战略”)，该战略的主要目标是建立“隐私保护机制健全、认证和识别技术标准、具有长期与广泛应用价值”的身份识别生态系统，以降低网络空间欺诈风险，抵御信息盗窃、篡改、伪造和非法利用。

2012年8月，美国成立了国家可信身份战略的指导小组，负责身份生态系统架构标准和认证过程的制定。国家计划办公室(National Program Office，NPO)负责协调战略实施过程中相关机构的工作流程、具体行动以及战略的日常协调工作，各州、地方和自治政府也参与到身份生态系统框架的建设中。目前该身份认证生态系统已率先在机动车辆管理员协会等组织内进行试点，且工作效果很好。美国计划3~5年内实现身份认证生态系统初步运营的一些关键目标，10年后，身份认证生态系统基本建成，主要优势完全体现。

美国NSTIC战略框架提出后，大部分西方国家都在学习借鉴美国的这种做法，日本、欧盟、新加坡等国家和组织先后颁布了互联网可信生态环境战略的相关文件和法律，2013年日本内阁下属的信息安全中心颁布了《网络安全战略》，欧盟则颁布了《欧盟网络安全战略：公开、可靠和安全的网络空间》，为欧盟网络空间的建设和管理提供规范和指导。

可以看到，当前在互联网建设领域领先的国家，已将注意力聚焦在如何保证网络行为的安全性和网络身份的真实性上，以建立基于身份识别系统的网络可信生态环境。

本书在系统调研美国等发达国家互联网可信生态环境的基础上，着重分析了我国互联网可信生态环境现状，提出了建设我国互联网可信生态环境的对策建议。我国互联网可信生态环境建设已具备一定基础，手机实名制、银行账户、指纹认证以及将启动的统一社会信用代码制度，都为网络身份认证提供了良好的社会基础，但不利条件是我国的社会诚信和社会信任体系尚未完全建立，因此还须率先发展社会信任体系建设。

目前我国主要存在的问题有：社会信用机制尚未完善；缺乏战略目标、规划和方案；管理体制和机制滞后。具体包括如下几个方面。

一是从国家层面还未形成明确的可信网络空间生态环境建设的战略目标和规划，缺乏一套完整的互联网可信生态环境框架方案。

二是我国实行多头和切块式网络管理，电子商务、金融、电信、网络媒体等各自为政，缺乏统一的认证体系和平台，身份认证、信用等级资源未实现共享，未形成完整的网络空间可信生态环境。切块式管理还容易造成职责不清，责任不明，“推诿”“扯皮”，利益多家抢，责任互相推等现象，还易形成无人管理的空白地带，这不仅增加了网络管理成本和难度，还造成了信息和资源

共享难、管理效率低等问题。在管理机制上，网络管理效果与政府官员绩效没太多关联，地方政府对网络管理缺乏重视和动力，也是网络管不过来、没法管的原因之一。

三是网络空间信用等级低。我国的社会诚信和社会信任体系尚未完全建立，网络信用机制更为缺失，网络欺诈、网络攻击、网络侵权与犯罪事件多发，网络秩序较为混乱。一方面，某些互联网公司出于商业利益和某种不法目的，掠取公民的个人隐私和信息，尤其是在那些外资已占很大份额甚至已控股的互联网公司，此种现象尤为严重，直接影响到网民的信息安全；另一方面，某些网民的不规范行为，很大程度上源于网络空间中网民权利与义务不对等，法律责任无法很好追溯。因此，建立可信身份认证机制，也可为网络责任的可追溯性提供途径。

四是我国信息领域相关法律法规严重滞后。主要表现为至今还没有信息领域内的根本大法，即大多数国家都有的《信息公开法》或《信息自由法》，也没有针对互联网和信息传播的具体法律，现有法律少，部门规章多，行政法规多，以及临时性的行政管理规定或带有决定性的文件多，惩戒力度低，法律效力和执行力大打折扣；现行法律法规框架性东西多，过于简单和笼统，缺乏操作细则，增加了执法难度。

我们对互联网生态环境建设的对策建议如下：

战略先行，详细规划，尽快启动可信网络空间生态环境建设，加强法治和管理，逐步形成线上线下一体化的信用环境体系。

一是从国家层面尽快形成可信网络空间生态环境建设的战略规划，建立一套完整的网络空间身份识别和生态环境框架方案。

1. 建立完善的隐私保护机制、规则和指南，明确服务提供商和依赖方共享信息的问题，并明确他们在什么情况下可以收集用户信息、可以收集用户哪类信息、这些信息如何被管理和使用等。中央政府行政部门与运营商共同制定规章制度以加强保护个人

隐私。

2. 在已有的风险模型的基础上制定广泛的认证和识别标准。

3. 定义身份认证系统中的参与者责任并建立问责制，确定系统中参与者的最低权利和责任。同时从法律层面界定互联网中各大主体，包括政府、企业、运营商、其他主体以及个人之间的关系、权益和责任。在网络空间可信生态环境建设中，政府发挥组织、引导、标准制定和监管职能，企业扮演的是生态链中的供应者，负责创建和维护身份验证、更新和撤销等属性。通过完善的监管机制、社会诚信体系和强大的数据资源，建立一套网络身份识别系统。

4. 建立一个指导小组，管理身份识别系统架构标准的制定和认证过程，制定管理政策和技术标准，按照战略规划的指导原则进行组织和引导。

二是尽快启动以可信身份认证机制、信用等级机制、信息共享机制为主体的网络空间可信身份识别环境建设。本书提出四种网络身份认证方式，分别如下。

（1）基于实名制手机验证码的身份认证方式；

（2）基于网银 U－Key 的身份关联认证方式；

（3）基于指纹特征的身份认证；

（4）基于网络电子身份证 eID 的身份认证。

建立互联网信任体系和信任分级制度，须先将各种不同的网络身份归结为唯一标识，最直接的方法就是将网络虚拟身份与现实身份关联起来，还原其社会身份。因此，可信的身份认证机制成为构建互联网可信生态系统的基础要素之一，在此基础上，建立用户的信任分级制度。笔者从基础条件、推行成本、技术难度、隐私保护、对用户心理冲击几方面对四种认证方式进行了分析，认为在我国现有互联网基础环境下，可以先从推行难度最小的手机验证码认证方式入手，使身份认证工作能够较快进行，同时积

极推广网络电子身份证 eID，逐步实现以 eID 代替手机作为认证介质的转化，以降低风险，提高认证效率。

三是加强加快信用体系相关法律法规建设，加强执法力度。2013 年开始的“净网行动”对于清理网络谣言，净化网络环境起到了非常有效的作用，但若要长治久安则须从法律上解决问题，依法治网。同时网络空间可信生态环境建设也要依法办事，依法执行。

四是建立统一的网络管理体制和机制，提高网络管理的级别和效率。尽快完成互联网运营商和用户责任的可追溯性，从而加强网络舆情的监控，加大对网络犯罪、网络谣言的打击力度，改善互联网空间秩序。

五是加快大数据建设工作。我国公民社会信用代码制度建设工作已经启动，这是加快全国大数据建设的最好时机，而互联网可信生态认证是基于大数据云的一项互联网可信管理技术，因此大数据建设工作关系到互联网可信生态系统的建设。

六是在建立互联网可信生态环境体系时，应注意与社会信用体系以及相关法规政策接轨，以求形成线上线下一体化的信用环境体系。网上身份认证、信任等级评价应与社会真实身份及信用评价一致，且进行信息关联，在建立网络身份认证的同时，大力发展完善我国的信任体系，加快推动互联网以及全社会可信生态系统的建设。

在课题调研和成果编撰过程中，陈持协、刘洋、白佐铭、黎文勇等人协助做了大量工作，同时，我们得到了诸多专家和领导的帮助与支持，在此表示感谢。

CONTENTS
目 录

第一部分 主要发达国家互联网可信生态环境

第二部分 我国互联网可信生态环境现状

第三部分 我国互联网生态环境建设

第一部分

主要发达国家互联网可信生态环境

互联网可信生态环境概念最早由美国提出。2011 年 4 月 15 日美国白宫公布《可信互联网空间身份标识国家战略》(《National Strategy for Trusted Identities in Cyberspace》，简称“NSTIC 战略”)，该战略的主要目标是建立“隐私保护机制健全、认证和识别技术标准、具有长期与广泛应用价值”的身份识别生态系统，以降低网络空间欺诈风险，抵御信息盗窃、篡改、伪造和非法利用。自互联网问世以来，由于网络空间存在的虚拟性和自由性，它在提供极度自由的同时，也使得网络诚信存在巨大漏洞。互联网可信生态系统是互联网未来发展的方向，主要包括互联网网络实名认证机制、互联网信息共享机制、互联网信用等级分级机制。

本部分首先通过对互联网霸主美国互联网可信生态系统的分析，来了解互联网可信生态系统的发展道路，同时调研了国外其他互联网发达国家及我国现有的互联网法律法规，目的在于从实际出发，通过现有的规章制度来明确建设互联网可信生态系统的宏观定位与实施步骤。

第一部分包括两个章节，第 1 章调研分析了美国现有互联网基础建设、互联网管理体制、NSTIC 战略文件，第 2 章主要是从政府政策层面入手调研了日本、新加坡、韩国、欧盟相关法律文件和政府政策手段。

美国 NSTIC 战略已具体界定了政府部门、私营机构以及其他主体在身份认证过程中扮演的角色和任务，明确了系统参与者责任并建立了问责机制。其中，私营机构负责具体身份生态系统的设计和运营；联邦政府负责支持私营机构的行动并进行监督，确保身份生态系统在互操作、安全、隐私保护等方面达到要求。

在对美国等发达国家互联网生态环境调研和分析的基础上，我们发现这些在互联网建设领域领先的国家，已将注意力聚焦在如何保证网络行为的安全性，网络身份的真实性，建立基于身份识别系统的网络可信生态环境。

第1章 美国互联网可信系统

美国人发明了一项改变世界的工具——互联网。互联网建成之后，美国在互联网技术和管理上不断积累和完善，形成了一系列行之有效的法律和管理手段。其基础设施建设、互联网管理机制和NSTIC法案对于我国的互联网可信系统建设都有重要的参考意义，其中互联网管理机制还包括美国现有的立法现状、技术监管、政府自律引导、市场调节、企业配合、信息共享等多个角度。

1.1 基础设施建设

1.1.1 基础设施的自主性与可控性

（1）互联网根域名服务器

互联网的安全可信来源于基础设施的自主性和可控性，美国作为互联网发源地，控制着互联网的主要命脉——根域名服务器。全世界共有13台根域名服务器，其中1台为主根服务器，放置在美国弗吉尼亚州的杜勒斯，其余12台为辅根服务器，有9台放置在美国，2台在欧洲，分别位于英国和瑞典，1台在亚洲，位于日本。美国控制了域名解析的根服务器，也就控制了相应的所有域名，如果美国不想让某些域名被访问，可以屏蔽掉这些域名，使它们的IP地址无法被解析出来，那么这些域名所指向的网站就相

当于从互联网的世界中消失了。2005 年 7 月 1 日，美国政府宣布，美国商务部将无限期保留对 13 台根域名服务器的监控权。例如，2004 年 4 月由于“.ly”域名瘫痪，导致利比亚从互联网上消失了 3 天。另外，凭借在域名管理上的特权，美国还可以对其他国家的网络使用情况进行监控，如美国可以对某个国家的某类网站进行流量访问统计，从中大致分析出该国热门网站分布情况和网民的访问喜好等[1]。

（2）通信设备巨头——思科

思科是美国互联网的宠儿，是 2003 年 3 月公布的“美国最佳企业”，这使思科一跃成为互联网时代的可信企业，作为通信设备的巨头，不断发展的思科完成了战略全球化。通过与政府的合作，思科为美国内部互联网的可信基础建设做出了重要贡献。美国政府曾通过思科获取的情报处理了很多国内甚至全球的欺诈、欺骗、非法网站，以及他国黑客攻击事件。

1.1.2 基础设施的保护机制

总统关键基础设施保护委员会（办公室）

总统关键基础设施保护委员会（办公室）是由美国政府各主要部门的内阁成员构成，其主要职能是为政府提供网络信息安全、基础设施安全、互联网可信生态环境状况等相关信息，同时该办公室还为美国相应政策提供咨询意见，并负责组织、协调各项信息安全计划的执行活动。

“9·11 事件”后，小布什总统发布第 13231 号总统令，将“关键基础设施保护委员会”这一协调机构改为行政实体——关键基础设施保护办公室，直接纳入总统办公厅的领导之下，重组后的关键基础设施保护办公室成员包括各相关主管部门的首长及总统的相关助理官员。

重组后的关键基础设施保护办公室主要承担以下职能[2]：