

——2012年度——

国家信息安全态势评估

National Cyber Security Review 2012

中国信息安全测评中心

时事出版社

——2012年度——

国家信息安全态势评估

National Cyber Security Review 2012

中国信息安全测评中心

时事出版社

图书在版编目 (CIP) 数据

2012 年度国家信息安全态势评估/中国信息安全测评中心编著.
—北京: 时事出版社, 2013. 4
ISBN 978-7-80232-611-8

I. ①2… II. ①中… III. ①信息安全—国家安全—研究—
中国—2012 IV. ①D631

中国版本图书馆 CIP 数据核字 (2013) 第 061950 号

出版发行: 时事出版社
地 址: 北京市海淀区巨山村 375 号
邮 编: 100093
发行热线: (010) 82546061 82546062
读者服务部: (010) 61157595
传 真: (010) 82546050
电子邮箱: shishichubanshe@sina.com
网 址: www.shishishe.com
印 刷: 北京百善印刷厂

开本: 787×1092 1/16 印张: 20.25 字数: 230 千字

2013 年 5 月第 1 版 2013 年 5 月第 1 次印刷

定价: 56.00 元

(如有印装质量问题, 请与本社发行部联系调换)

序

回顾 2012 年，信息网络正逐步成为现代国家的“神经中枢”。虚拟网络与现实社会互动交织，深度和广度空前。就国家信息安全而言，从黑客猎奇、地下产业链到高智能犯罪，从个人隐私、商业秘密到国家机密泄露，从个人攻击、团体攻击到国家网络攻击，从网络谣言、群体事件到街头政治颠覆政权等等，万象丛生，错综复杂。信息安全早已不是单纯的技术问题，而是可能牵动社会思潮、国家中枢、乃至国际安全态势演变的无形之手。

透过世界各国安全战略调整和网络备战的硝烟，我们看到网络空间的利益争夺和较量更趋激烈。纵观信息泄露、网络犯罪、激进黑客行为、高发网络谣言、火焰病毒、华为中兴“安全门”争端等涉网事件，我们看到信息安全形势严峻复杂。我国重要信息系统、工业控制领域的风险依然居高难下，安全与发展的矛盾交织，网络空间的战略地位及信息安全的重要程度空前提高。在

这样的现实情况下，如何科学利用好信息资源，依法管理好网络空间，不仅是我国信息化发展亟需解决的问题，也是当前世界各国共同面临的治理难题。

可喜的是，我国的信息安全保障体系建设稳步推进，经受住了一年的风雨考验。各主管部门精心组织部署，有效管控风险；技术职能机构发挥专业特长，消除安全隐患；各行各业强化安全防范，推进网络发展，在日益攀升的安全风险中确保了各重要网络系统运行正常，总体态势基本平稳。《关于大力推进信息化发展和切实保障信息安全的若干意见》和《关于加强网络信息保护的決定》的发布，为强化信息安全管理，推进依法管理网络，又增添了浓重的一笔，意义非同寻常。

2013 年，面对国内外依然严峻的信息安全威胁与挑战，我们亟待进行思路上的转变、策略上的调整、重点的转移和战略的升级，以网络的方式应对安全挑战、以国际规则出好中国的牌、以安全保障力促网络发展、以顶层设计引导管理的创新，使我国的信息安全管理真正步入一个依法治理、科学发展的新阶段，乘“十八大”春风，在新的历史起点上，开创国家信息安全保障工作的新局面。

吴世忠

2013 年 2 月

北京·中关村·上地

主 编：吴世忠

编 委 会：吴世忠 武 轶 李守鹏 江常青

霍海鸥 王 军 沈敦厚 李 斌

刘 晖

主要撰稿人(按姓氏笔画排序)：

王 庆 卢英佳 伊胜伟 刘作康

刘彦钊 刘 星 刘洪梅 毕海英

张 利 张翀斌 张 舒 李 婧

李 森 陈海强 施 蕾 赵向辉

徐长醒 郭 涛 高 洋 彭 勇

董国伟



图表目录

图表 1: 电子政务信息孤岛示意图	(89)
图表 2: 电子政务未来发展方向	(93)
图表 3: 2012 年 1 至 12 月份我国网站被篡改报警次数 按月度统计	(113)
图表 4: 2012 年 1 至 12 月份我国网站被篡改报警次数 按区域分布示意图	(113)
图表 5: 2012 年 1 至 12 月份我国政府网站被篡改情况 按月度统计	(114)
图表 6: 2012 年 1 至 12 月份我国被挂马网页数量按月度 统计 (单位: 个)	(115)
图表 7: 2012 年 1 至 12 月份我国被挂马网站数按地域 分布示意图	(118)
图表 8: 2012 年 1 至 12 月份我国被挂马网站数按地域 分布统计	(119)

图表 9: 2012 年 1 至 12 月份我国被挂马网站按域名

分类统计 (120)

图表 10: 2012 年 1 至 12 月份我国被挂马网站按域名按月份

的分类统计 (121)

图表 11: 已确认的钓鱼网站的数量按照月份统计情况

示意图 (122)

图表 12: 对钓鱼欺诈网站的拦截情况的月度统计

示意图 (122)

图表 13: 2012 年 1 至 12 月份我国钓鱼网站类别分布

示意图 (123)

图表 14: 2012 年 1 至 12 月份网站暗链关键词 TOP10 统计

示意图 (125)

图表 15: 2012 年 1 至 12 月份我国常见域名被暗链攻击的

统计情况示意图 (126)

图表 16: 2012 年 1 至 12 月份我国范围内按恶意文件数量

统计情况 (攻击次数的单位: 万) (127)

图表 17: 2012 年 1 至 12 月份我国范围内恶意终端攻击中

被攻击用户数量统计 (单位: 万) (127)

图表 18: 2012 年 1 至 12 月份我国范围内恶意终端攻击中

被攻击用户 IP 分布统计 (128)

图表 19: 2012 年 1 至 12 月份我国范围内恶意终端攻击中

被攻击用户 IP 分布示意图	(128)
图表 20: 舆情热点分类统计	(152)
图表 21: 舆情热点地域分布	(153)
图表 22: 供应商提供的应用程序	(194)
图表 23: 供应商提供的业务关键性应用程序	(195)
图表 24: 各类供应商提供的应用程序在初次提交测试时 的表现 (* 小样本量)	(197)
图表 25: 供应商初次提交的版本符合 OWASP Top10 的情况 (WEB 应用程序)	(198)
图表 26: 供应商初次提交的版本符合 CWE/SANS Top25 的情况 (非 WEB 应用程序)	(199)
图表 27: 供应商重新提交应用程序的比例	(200)
图表 28: 各行业再次提交应用程序的比例	(201)
图表 29: 各种业务关键性应用程序的再次提交比例	(202)
图表 30: 应用程序各个版本的安全质量分数	(203)
图表 31: 安全质量分数在各季度的指数	(204)
图表 32: 各类供应商达到可接受的安全质量所需时间 ...	(205)
图表 33: 要求第三方风险评估的组织在各行业中的 分布情况	(207)
图表 34: 第三方评估在各种用途的应用程序中的 分布情况	(208)

图表 35: WEB 和非 WEB 应用程序分布	(209)
图表 36: 应用程序开发语言的分布	(210)
图表 37: 漏洞类型排名 (在网络应用程序中的总体 流行度)	(211)
图表 38: 漏洞类型排名 (在非网络应用程序中的总体 流行度)	(212)
图表 39: 漏洞类型排名 (网络应用程序被感染 的比例)	(213)
图表 40: 漏洞类型排名 (非网络应用程序被感染 的比例)	(214)
图表 41: 跨站脚本按季度指数	(215)
图表 42: SQL 注入按季度指数	(216)
图表 43: Android 应用程序在各垂直产业中的 分布情况	(219)
图表 44: 各项安全评估的分数分布情况	(221)
图表 45: 参加各课程的学生的分布情况	(222)
图表 46: 各省市获证企业分布情况	(239)
图表 47: 二级获证企业分布情况	(240)
图表 48: 2007 至 2012 年漏洞新增数量统计图.....	(254)
图表 49: 2012 年全年漏洞分布情况	(255)
图表 50: 2007 至 2012 年主流操作系统漏洞概况.....	(257)

图表 51: 2007 至 2012 年 Web 浏览器漏洞数量统计	(258)
图表 52: 2012 年 Web 浏览器漏洞数量统计	(258)
图表 53: 2007 至 2012 年主要漏洞类型逐年 变化趋势	(260)
图表 54: 2012 年漏洞危害等级分布	(261)
图表 55: 2007 至 2012 年漏洞严重等级分布	(261)
图表 56: 2007 至 2012 年漏洞利用复杂性	(262)
图表 57: 2012 年漏洞修复数量统计	(263)
图表 58: 2007 至 2012 年 10 大厂商漏洞数量 变化情况	(268)
图表 59: 2007 至 2012 年 Java 漏洞数量增长情况	(269)
图表 60: 2007 至 2012 年 Web 浏览器漏洞概况	(270)
图表 61: 2007 至 2012 年 Android 漏洞数量统计	(271)
图表 62: 2007 至 2012 年漏洞修复情况	(271)
图表 63: 2007 至 2012 年厂商漏洞修复率	(272)
图表 64: 2012 年工控系统漏洞数量按品牌分布	(278)



目 录

第一章 2012 年度国内外信息安全

总体态势 (1)

一、2012 年国际信息安全总体态势 (2)

二、2012 年国内信息安全总体态势 (24)

三、2013 年国内外信息安全形势 (39)

第二章 国外主要国家和地区信息

安全态势 (48)

一、美国信息安全态势 (49)

(一) 战略层面：加强网战力量和能力建设，加紧

网络军事扩张 (49)

(二) 政府层面：调整内政外交政策，借网络安全

问题频频施压	(53)
(三) 产业技术层面: 重视国内资源整合, 政企共同 应对网络威胁	(57)
(四) 国际影响: 强调互联网国际合作, 建立全球性 的多利益相关方合作机制	(58)
二、俄罗斯信息安全态势	(60)
(一) 战略层面: 合纵连横, 抢占网络空间控制权 ...	(60)
(二) 政府层面: 进一步加强网络防御体系建设	(61)
(三) 产业技术层面: 大力发展自主创新信息 安全技术	(63)
(四) 国际影响: 遏制与合作并存	(64)
三、欧洲信息安全态势	(65)
(一) 战略层面: 进一步加强网络防御体系和机制 机构建设, 积极制订网络政策	(66)
(二) 政府层面: 采取多种管理措施, 防范网络攻击 及网域犯罪	(68)
(三) 产业层面: 政企合作, 增强信息产业核心 竞争力	(70)
(四) 国际影响: 开展互联网国际交流与合作, 保障跨境网络安全	(71)
四、亚洲各国信息安全态势	(73)

(一) 印度: 加强与日本合作, 安全竞争态势突出 …	(73)
(二) 韩国: 加强网络攻击能力建设	(75)
(三) 日本: 调整网络空间安全战略, 全面提升网络 攻击能力	(78)
(四) 菲律宾: 加强个人隐私保护, 促进电子商务 产业发展	(80)
(五) 伊朗: 进一步收紧网络审查制度, 加快建立 国家互联网	(80)
(六) 中亚其他国家: 加强对新媒体的管控	(81)

第三章 我国电子政务、基础网络和重要

信息系统安全态势

一、我国电子政务信息系统安全保护情况

(一) 基本情况与安全现状

(二) 隐患分析与风险评估

(三) 态势预测与对策建议

二、我国基础信息网络和重要信息系统

安全态势

(一) 基本情况与安全现状

(二) 主要问题与安全隐患

(三) 效能性能

（四）态势预测与对策建议·····	（105）
-------------------	-------

第四章 我国互联网安全形势·····（110）

一、互联网安全事件概况·····	（111）
------------------	-------

（一）互联网安全状况统计·····	（112）
-------------------	-------

（二）主要问题分析·····	（129）
----------------	-------

（三）对策建议·····	（134）
--------------	-------

二、互联网内容安全状况·····	（136）
------------------	-------

（一）主要典型舆情热点点评·····	（137）
--------------------	-------

（二）舆情典型特征分析·····	（150）
------------------	-------

（三）舆情安全对策建议·····	（161）
------------------	-------

第五章 我国信息安全产业现状及

产品动态·····	（164）
-----------	-------

一、现状及趋势分析·····	（165）
----------------	-------

（一）信息安全产品市场现状及趋势分析·····	（165）
-------------------------	-------

（二）主流信息安全产品现状及趋势分析·····	（166）
-------------------------	-------

二、综合评估·····	（178）
-------------	-------

（一）效能性能评估·····	（179）
----------------	-------

（二）风险评估·····	（181）
--------------	-------

三、对策建议	(182)
--------------	-------

第六章 我国主流软件信息安全态势

(184)

一、主流软件的应用及安全态势	(185)
----------------------	-------

(一) 主流软件的应用情况	(185)
---------------------	-------

(二) 主流软件的安全问题	(187)
---------------------	-------

(三) 对策建议	(190)
----------------	-------

二、软件安全性评估	(192)
-----------------	-------

(一) 基于软件供应链的安全现状分析	(193)
--------------------------	-------

(二) 应用程序的安全性	(209)
--------------------	-------

(三) 开发者培训和教育	(220)
--------------------	-------

(四) 威胁趋势	(222)
----------------	-------

第七章 我国信息安全服务及从业

人员情况	(227)
------------	-------

一、信息安全服务发展情况	(228)
--------------------	-------

(一) 我国信息安全服务产业总体状况	(228)
--------------------------	-------

(二) 信息安全服务存在的主要问题	(237)
-------------------------	-------

(三) 解决当前问题的有效途径及建议	(242)
--------------------------	-------

二、信息安全从业人员状况	(244)
--------------------	-------

（一）国外信息安全人员动态·····	(244)
（二）我国信息安全从业人员状况·····	(248)
（三）对策建议·····	(251)

第八章 我国信息安全漏洞情况 ····· (253)

一、安全漏洞增长概况 ·····	(254)
二、安全漏洞分布 ·····	(255)
（一）厂商漏洞分布·····	(255)
（二）产品漏洞分布·····	(256)
（三）漏洞类型分布·····	(259)
（四）漏洞危害等级分布·····	(260)
三、安全漏洞危害与修复 ·····	(262)
（一）安全漏洞利用与修复性·····	(262)
（二）漏洞修补情况·····	(262)
四、本年度重要漏洞实例分析 ·····	(264)
五、本年度漏洞特点及趋势分析 ·····	(268)

第九章 我国重大信息技术及应用的

安全评估 ····· (274)

一、我国工控系统信息安全态势 ·····	(275)
----------------------	-------