

中国域名服务安全状况与态势分析报告

· 2014 ·



目录

专业术语表.....	3
1、 前言.....	5
2、 摘要.....	7
3、 域名服务安全状况.....	8
3.1 根域名服务系统.....	8
3.1.1 简介.....	8
3.1.2 系统软件.....	9
3.1.3 协议支持.....	9
3.1.4 服务性能.....	10
3.2 顶级域名服务系统.....	12
3.2.1 简介.....	12
3.2.2 系统软件.....	12
3.2.3 协议支持.....	12
3.2.4 服务性能.....	13
3.3 二级及以下权威域名服务系统.....	15
3.3.1 简介.....	15
3.3.2 系统软件.....	15
3.3.3 协议支持.....	16
3.3.4 服务性能.....	16
3.3.5 国内二级及以下权威域名服务系统.....	18
3.3.6 国内重点权威域名服务系统.....	21
3.4 递归域名服务系统.....	25
3.4.1 简介.....	25
3.4.2 系统软件.....	25
3.4.3 协议支持.....	25
3.4.4 服务性能.....	26
3.4.5 国内递归域名服务系统.....	27
3.4.6 国内主要递归域名服务系统.....	30
4、 域名服务安全评估.....	34
4.1 权威域名服务系统.....	34
4.2 递归域名服务系统.....	36
5、 我国域名基础设施安全态势分析.....	38

专业术语表

缩略语	英文全称	中文全称
ccTLD	Country Code Top Level Domain	国家与地区顶级域名
CDN	Content Delivery Network	内容分发网络
DNS	Domain Name System	域名系统
DNSSEC	DNS Security Extensions	域名系统安全扩展
DoS	Denial of Service	拒绝服务攻击
gTLD	General Top Level Domain	通用顶级域名
IANA	Internet Assigned Numbers Authority	互联网数字分配机构
ICANN	Internet Corporation for Assigned Names and Numbers	互联网名称与数字地址分配机构
IPv4	Internet Protocol version 4	互联网协议第四版本
IPv6	Internet Protocol version 6	互联网协议第六版本
ISC	Internet Software Consortium	互联网系统协会
TCP	Transmission Control Protocol	传输控制协议
TLD	Top Level Domain	顶级域名
TTL	Time To Live	生存时间

1、前言

域名系统是支撑目前绝大多数互联网应用的互联网基础设施中的关键环节。域名服务安全是互联网安全的重要组成部分；没有域名服务安全，就没有整个互联网的安全。域名服务体系涵盖提供域名服务的所有域名系统，由两大类别、四个环节组成：第一类是权威域名解析服务系统，包括根域名服务系统、顶级域名服务系统和其他各级域名服务系统三个环节。权威域名服务系统由各级域名持有者管理，负责维护和保存各级权威域的域名信息，并且接受递归服务器的查询请求。第二类是递归域名解析服务系统，它们面向终端用户提供域名查询服务。具体架构如图 1 所示。

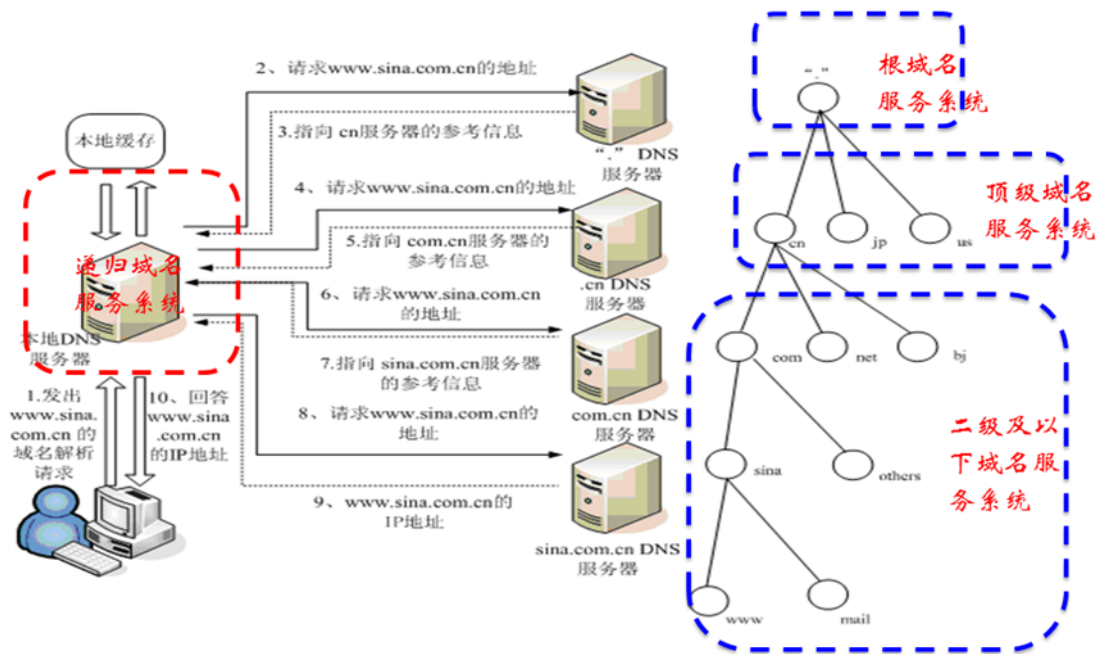


图 1 域名服务体系的构成

对我国域名基础设施网络安全的监测一方面有助于对我国域名系统安全状态进行完整、精确、深入的把握，另一方面也可以借助于域名系统安全状况进行我国互联网安全态势的分析和评估。

自 2009 年起，中国互联网络信息中心（以下简称 CNNIC）就开始对整个域名服务体系的配置情况和安全态势进行多角度的监测分析。为了对域名服务体系的运行状态和安全情况进行更为准确、客观的了解，基于 CNNIC 自建的国家域名安全监测平台，在全球范围内部署了广泛的监测节点。平台通过故障、配置、

性能和流量等多角度的监测，对根域名服务系统、顶级域名服务系统、二级及以下权威域名服务系统和递归域名服务系统的运行状态和安全状况进行全面监测和客观评估。

2、摘要

2014 年我国域名服务体系主要情况如下:

- 1) 各级域名服务器采用 Linux/Unix 操作系统的比例均高于 80%，使用 ISC BIND 域名解析软件的比例均在 90% 以上，但是超过 30% 的各级域名服务器所使用的 BIND 软件仍然支持版本应答，存在一定安全隐患；
- 2) 根域名服务系统对于 DNSSEC、IPv6、TCP 等相关协议的支持程度最高，同比新增 61 个镜像节点，平均解析速度同比提升 20%；
- 3) 顶级域名服务系统的相关协议支持程度同比有了进一步加强，其中 DNSSEC 支持率大幅提升至 78%，服务冗余程度进一步加强，大量新通用顶级域名开始对外服务；
- 4) 二级及以下权威域名服务系统在相关协议支持程度方面提升有限，但在服务冗余程度方面有较为明显的改善；对于国内二级及以下权威域名服务系统，相关协议支持程度明显相对不足，但服务冗余程度及平均解析速度相对较高；
- 5) 递归域名服务系统在 DNSSEC 支持方面仍然较低，大数据包支持比率进一步提升；
- 6) 总体而言，我国域名服务整体安全状况稳中有升，有少量域名服务的安全问题依然突出。

3、域名服务安全状况

3.1 根域名服务系统

3.1.1 简介

域名服务系统通过层次化的形式管理域名数据，从而以分阶段的方式将人们可以记住的域名转换为计算机使用的数字以寻找其对应的目的地。根域名服务系统作为提供域名权威数据的入口，其服务器数量和分布对互联网域名解析服务性能和安全稳定有很大的影响。截至 2014 年 12 月 31 日，域名系统 13 个根服务器在全球的镜像节点数量共 447 个(较去年同期新增 61 个)，其中中国大陆依然拥有 F 根、I 根、J 根和 L 根的镜像共计 6 个镜像节点。

根服务器的运营管理者及对应的 IP 和 AS 号如表 1 所示。

表 1 根服务器主要情况¹

根服务器	运营者	IP地址	AS号
A	VeriSign, Inc.	IPv4: 198.41.0.4 IPv6: 2001:503:BA3E::2:30	26415
B	University of South California -Information Sciences Institute	IPv4: 192.228.79.201 IPv6: 2001:478:65::53	4
C	Cogent Communications	IPv4: 192.33.4.12 IPv6: 2001:500:2::C	2149
D	University of Maryland	IPv4: 199.7.91.13 IPv6: 2001:500:2D::D	27
E	NASA Ames Research Center	IPv4: 192.203.230.10	297
F*	Internet Systems Consortium, Inc.	IPv4: 192.5.5.241 IPv6: 2001:500:2f::f	3557
G	U.S. DOD Network Information Center	IPv4: 192.112.36.4	5927
H	U.S. Army Research Lab	IPv4: 128.63.2.53 IPv6: 2001:500:1::803f:235	13
I*	Netnod	IPv4: 192.36.148.17 IPv6: 2001:7fe::53	29216
J*	VeriSign, Inc.	IPv4: 192.58.128.30 IPv6: 2001:503:C27::2:30	26415

¹ 注：“*”表示在中国境内具有该服务器镜像节点。

K	RIPE NCC	IPv4: 193.0.14.129 IPv6: 2001:7fd::1	25152
L*	ICANN	IPv4: 199.7.83.42 IPv6: 2001:500:3::42	20144
M	WIDE Project	IPv4: 202.12.27.33 IPv6: 2001:dc3::35	7500

3.1.2 系统软件

监测显示，根域名服务器均采用了 Linux 或者 Unix 操作系统；DNS 服务软件方面，所有的根域名服务器同样都采用了 ISC BIND 软件。系统软件配置管理相对非常完善，表现出极高的服务管理能力。

3.1.3 协议支持

随着网络攻击技术的发展及 DNS 漏洞的频繁出现，攻击者已经大大缩短了劫持 DNS 查找过程的任一步骤所需的时间，从而可以更快地取得对会话的控制以实施某种恶意操作。若要在长期内消除此漏洞，唯一的解决方案是以端到端的形式部署 DNSSEC 协议。开发 DNSSEC 技术的目的之一是通过 DNS 数据进行数字签名来抵御此类攻击，从而使用户确信所接收到的数据有效。但是，为了从互联网中彻底消除该漏洞，必须在从根区到最终域名的查找过程中的每一步部署 DNSSEC。

因此，作为 DNSSEC 信任链的根源，根服务器是否支持 DNSSEC 对于整个 DNS 服务体系部署 DNSSEC 至关重要。检测结果显示，根服务器都已经部署了 DNSSEC 服务（ICANN 于 2010 年已宣布，根区完成 DNSSEC 签名）。数据加密算法为 RSA/SHA-256。此外，所有的根服务器都支持 NSEC。

IPv6 的普及离不开 DNS 对 IPv6 的支持。2014 年，C 根服务器开始支持 IPv6 服务，目前还有 E、G 节点仍未支持 IPv6。随着 DNSSEC、IPv6 地址的推广使用，DNS 应答数据包将逐步增大。在 IPv4 到 IPv6 的过渡期间，还会存在某些域名服务同时使用 IPv6、IPv4 地址的情况。而传统 DNS 数据包大小被控制在 512Byte 以下，通过一个 UDP 数据包进行传输，无法满足上述数据包的传输需求。因此，DNS 服务器在交换超过 512Byte 的数据时应开启 EDNS0 支持，或采用 TCP 代替 UDP。检测结果显示，所有的根服务器都支持 TCP 协议。

图 2 显示的是根域名服务器的协议支持比例分布情况。可见，根域名服务器在协议支持程度方面，除 C 根新增 IPv6 支持以外，与去年相比没有其他变化。

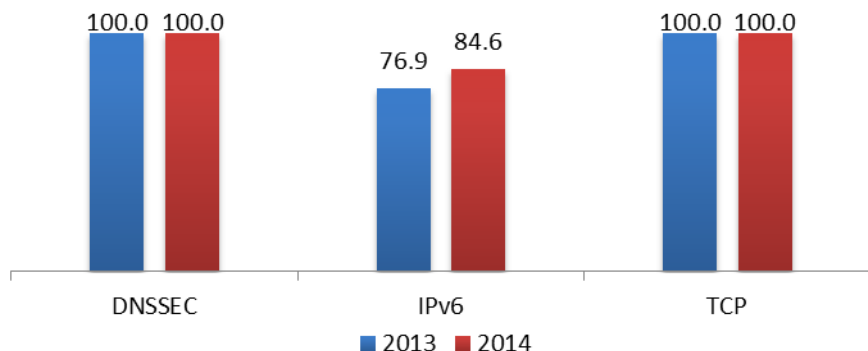


图 2 根域名服务器协议支持比例情况 (%)

3.1.4 服务性能

为了保证全球 DNS 服务的高可用性以及抗攻击能力，根服务器采用 BGP Global AnyCast 技术在全球范围内广泛部署镜像节点。截至 2014 年 12 月 31 日，全球共有 447 个根服务器镜像节点(较去年同期新增 61 个)，除了由 Information Sciences Institute 运维的 B 根以外，其他 12 个根服务器均在全球范围内部署了广泛的镜像节点。图 3 所示为 13 个根服务器各自所部署的镜像数量分布情况。

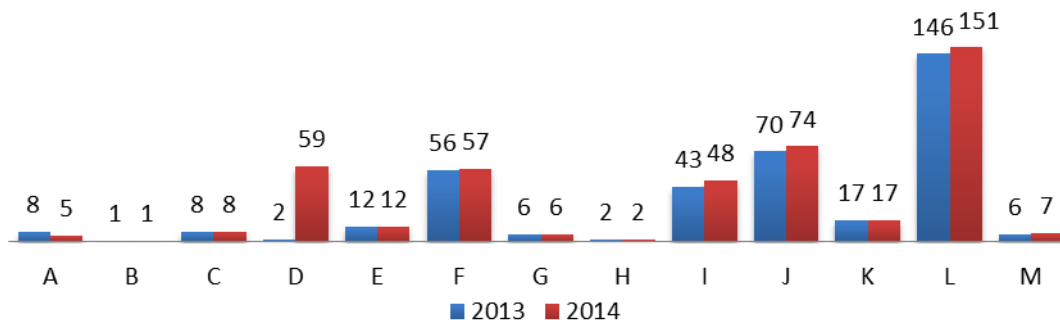


图 3 根服务器部署镜像数量分布情况

根域名服务系统采用 BGP Global AnyCast 机制保证多个镜像节点对于用户访问的透明性，该机制会将用户的 DNS 查询引导到距其最近的 DNS 根镜像节点，从而起到了一定的负载均衡作用。因此，根服务器查询时延的大小对于监测点的位置有直接的依赖性。为了全面反映国内互联网用户访问根服务器的时延，本报告对分布在全球范围内的监测点的探测结果取平均值，具体结果如图 4 所示。为了进一步监测国内互联网用户访问根服务器时延变化趋势，本报告记录了 2014

年3月起13个根服务器的平均探测时延，具体结果如图5所示（注：图5是每5分钟探测一次，探测频率、时延数据总量高于图4的定期监测）。从图4、图5可以看出，大部分根域名服务器的查询时延较去年都有了一定程度的减少，2014年7月份之后我国互联网连接根服务器的平均响应速度有所提升。

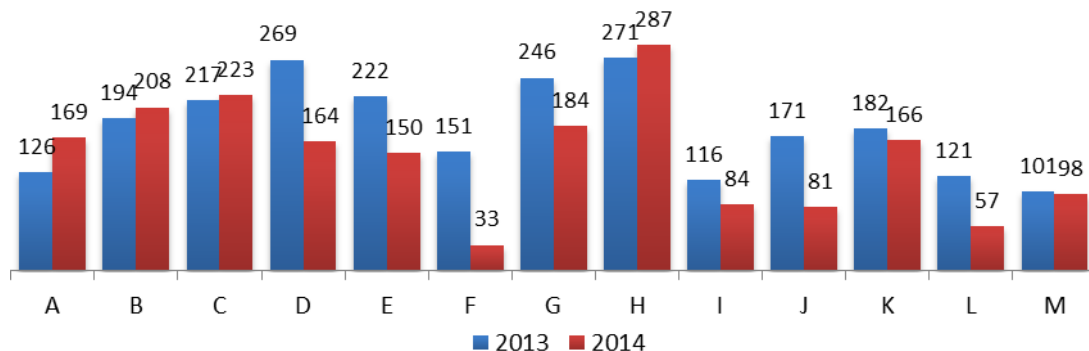


图4 根域名服务器查询时延分布情况（毫秒）

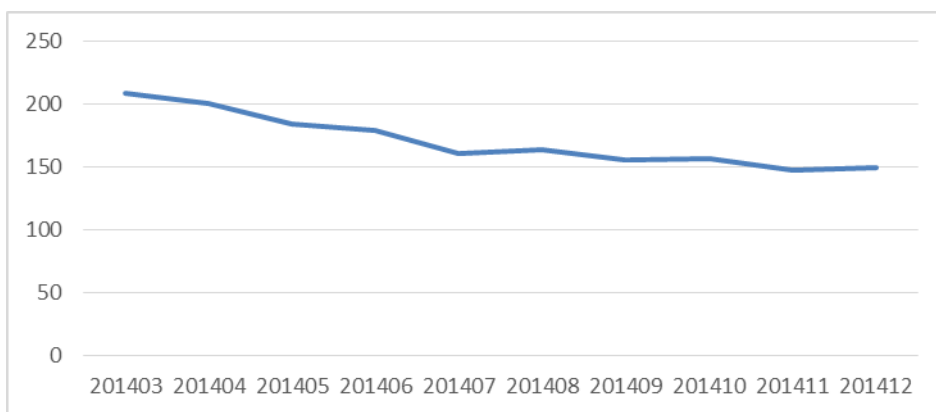


图5 根域名服务器平均查询时延趋势（毫秒）

中国早在2003年就引入了第一个根服务器的镜像—F根镜像，这是由ISC和中国电信共同建立的。2005年，I根的管理机构Autonomica（现已并入Netnod）在CNNIC设立了I根镜像。2006年，原中国网通（现已并入中国联通）与美国Verisign公司正式开通中国的J根镜像。此外，CNNIC于2012年与ICANN合作部署了国内第一个L根镜像，2014年天地互连和北龙中网又分别部署了L根镜像。这4个根服务器的6个镜像成为我国境内DNS查询请求最主要的根域名服务节点。

从图4中也可以看出，相对于其他根服务器，上述4个在国内拥有镜像的根服务器的查询时延相比其他根服务器明显要小，这表明根镜像在国内的部署确实可以有效提升我国境内查询根服务器的响应速度。

3.2 顶级域名服务系统

3.2.1 简介

根据国际互联网域名体系的构成，当前顶级域名共包含四类：通用顶级域名（gTLD）、国家与地区顶级域名（ccTLD）、基础设施类顶级域名（infrastructure，目前仅有.arpa）和实验性顶级域（test）。其中通用顶级域 gTLD 可细分为组织主办类（sponsored），通用类（generic），及限制通用类（generic-restricted）。根据 IANA 的统计，截至 2014 年 12 月 31 日，全球域名服务体系共包含 805 个 TLD，同比增长 110.2%，（去年同期 TLD 数量为 383 个），其中绝大部分是新通用顶级域（New gTLD）。

3.2.2 系统软件

监测显示，顶级域名服务器普遍采用了 Linux 或者 Unix 操作系统，两者所占比例达到 98% 以上。在所采用的 DNS 服务软件方面，ISC BIND 依然是绝大多数顶级域名服务器首选的 DNS 服务软件，比例占到了 81.8%，较去年略有下降（去年比例为 95.9%）。同时，采用 NLnetLabs NSD 软件的顶级域名服务器比例有了明显的提升，比例占到了 15.8%。32.6% 的 BIND 软件开启了版本应答功能（相比去年降低 5.5 个百分点），存在一定的安全隐患，应当引起相关运营方的重视。

3.2.3 协议支持

顶级域名服务器的协议支持分布情况如图 6 所示。可见，和去年相比，顶级域名服务器在协议支持方面有了全面的改善。

随着业界对于 DNSSEC 的努力推动，各顶级域名管理机构陆续开始部署 DNSSEC 服务。截至 2014 年 12 月 31 日，已有 78.0% 的顶级权威域部署了 DNSSEC，与去年相比大幅提升了 31.6 个百分点。其中所支持的加密算法，以 RSA/SHA-256 和 RSASHA1-NSEC3-SHA1 为主，两者占到了 91.4%。依然采用传统的 NextSECure（NSEC）机制的 DNSSEC 顶级域名服务器比例占到了 13.3%

（相比去年下降了接近 13 个百分点），具有区文件被遍历、枚举从而泄露所管理的域名解析数据的风险。

IPv6 支持比率由去年的 58.9% 提升到今年的 66.3%，TCP 支持比率由去年的 92.1% 增至 98.1%，这种变化有助于加速下一代互联网的过渡进程。

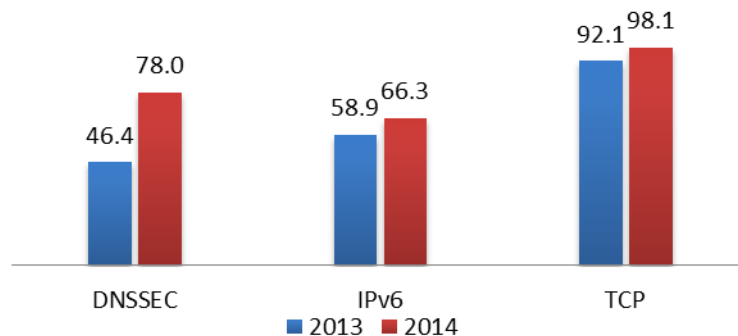


图 6 顶级域名服务器协议支持程度分布情况（%）

3.2.4 服务性能

监测显示，顶级域名服务器均具有冗余配置²，平均每个顶级域所拥有的服务地址数量由去年的 5.2 个大幅提升至今年的 7.6 个，其中超过半数的顶级域名服务器拥有超过 7 个服务地址，表现出极高的冗余性，具体情况如图 7 所示。

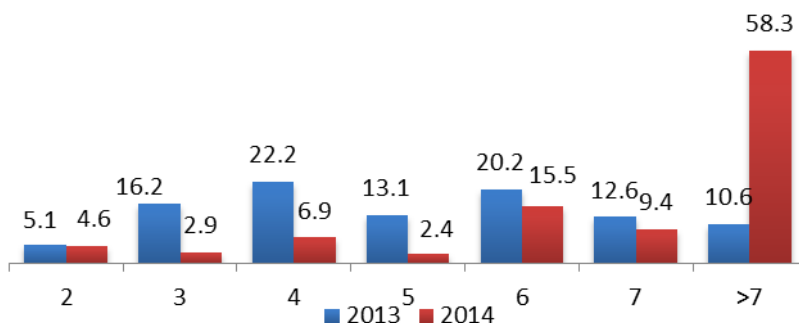


图 7 顶级域名服务地址数量比例分布情况（%）

权威域名服务器开启递归服务具有易遭受 DoS 攻击的风险。监测显示，顶级域名服务器的递归服务开启比例依然保持在较低的水平（0.52%）。

部署多台权威域名服务器能够起到增强权威域名服务鲁棒性和抗攻击能力的效果。但检测显示，6.1% 的顶级域名具有数据不一致的问题（去年同期该数值为 15.5%），即同一个顶级域的多台权威域名服务器数据不完全相同，这将会导

² 注：本报告以一个顶级域所具有的服务地址数量表示其冗余性程度。

致客户端从不同服务器查询得到不一致的 DNS 信息³。

服务器如果设置较大的 TTL，有可能会使客户端接收到过期的 DNS 缓存数据，但如果 TTL 设置过小，权威域名服务器将会因为频繁的 DNS 更新和区传输导致较大的开销，顶级权威域的 TTL 设置分布如图 8 所示。可以看出，有一定比例的顶级域名服务器开始倾向于选择较大的 TTL 值。

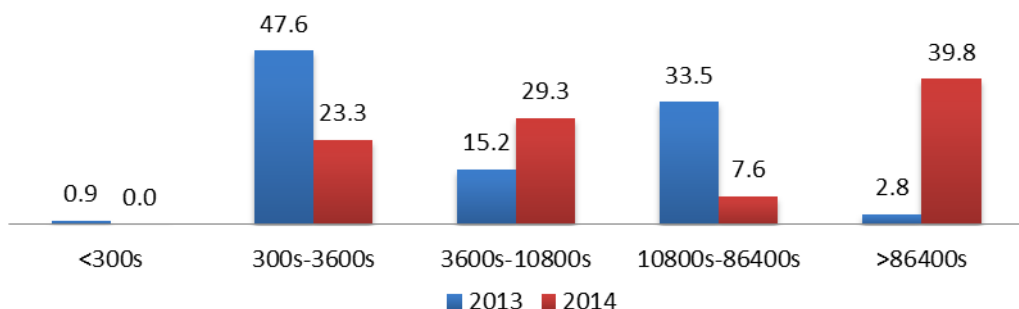


图 8 顶级域的 TTL 设置比例分布情况 (%)

由于顶级域名服务器的运维和管理都相对成熟，不仅整体配置和功能实现较为完善，服务状态良好。顶级域名服务器的查询时延分布如图 9 所示。可以看出，顶级域名服务器的整体查询时延相比去年有了较大的提升，超过 80% 的顶级域名服务器的查询时延在 0.5 秒以内。

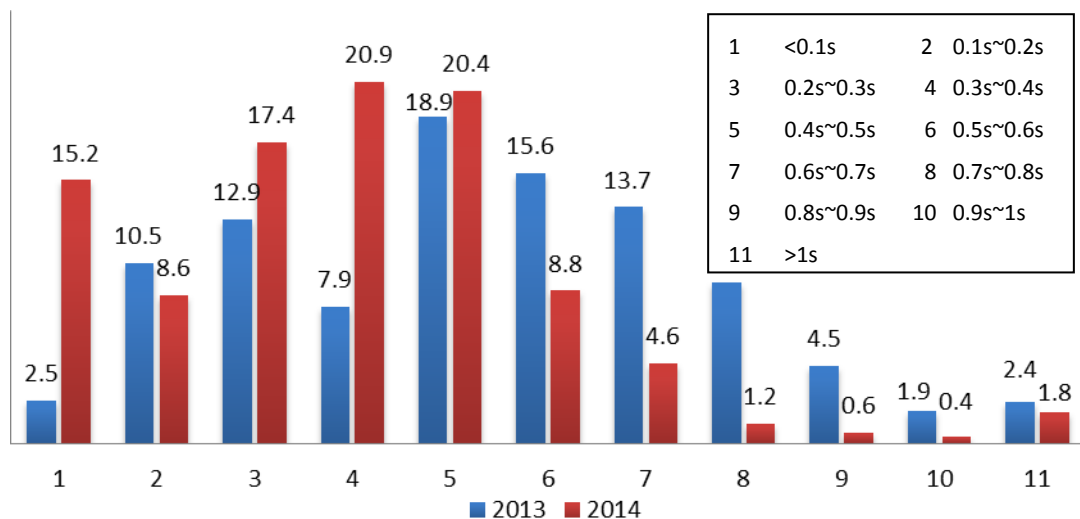


图 9 顶级域名服务器查询时延比例分布情况 (%)

³ 注：不排除检测时发生区传输等影响区数据的操作。

3.3 二级及以下权威域名服务系统

3.3.1 简介

二级及以下权威域名服务系统的基础建设普遍比较薄弱，运维能力也参差不齐。而其中一些域名服务器，如运行重点域名的服务器或运行重要信息系统的域名服务器，其所提供的权威数据直接影响到各种互联网应用的正常服务，一旦发生问题后果非常严重。为了抽样了解二级及以下权威域名服务系统的安全状态，本报告抽样选择了在中国境内使用最广泛的.CN、.COM 和.NET 三大顶级域下超过 1000 万个二级及以下域名作为监测对象，以下是详细的监测结果。

3.3.2 系统软件

Linux/Unix 为二级及以下权威域名服务器使用的主流操作系统类型，所占比例高达 85.4%，和去年基本持平（去年比例为 85.9%）。ISC BIND 在所有 DNS 软件中所占比例依然保持绝对领先，为 91.28%。具体分布如表 2 所示。此外，30.1%的 BIND 软件仍旧开启版本应答功能（去年该比例为 28%），存在一定的安全隐患。

表 2 二级及以下权威域名服务器 DNS 软件比例分布情况

软件类型	2013年所占比例（%）	2014年所占比例（%）
ISC BIND	91.45	91.28
DJ Bernstein TinyDNS	4.64	4.30
bboy MyDNS	2.58	1.96
JHSOFT simple DNS plus	0.5	0.9
Microsoft Windows DNS 2000	0.33	0.37
PowerDNS	0.09	0.14
UltraDNS	0.06	0.08
Nominum ANS	0.04	0.03
Microsoft Windows DNS 2003	0.03	0.56
NLnetLabs NSD	0.02	0.12
Other	0.26	0.26

3.3.3 协议支持

监测显示，虽然根域和顶级域的 DNSSEC 部署已经比较广泛，但是二级及以下权威域中仅有 0.33% 部署了 DNSSEC 服务（去年该比例为 0.26%），这也是整个 DNS 业界期望整体实现 DNSSEC 功能、避免安全孤岛的工作重点所在。对于已经签名的区域，同样以 RSA/SHA-256 和 RSASHA1-NSEC3-SHA1 为主，两者占到了 92.8%。依然采用传统的 NSEC 机制的 DNSSEC 权威服务器比例由去年的 4.1% 进一步缩减至今年的 3.5%，域名解析数据的泄露风险有所降低。

二级及以下权威域名服务器的协议支持比例情况如图 10 所示。可以看出，二级及以下权威域名服务器的整体协议支持比例情况有所提升。

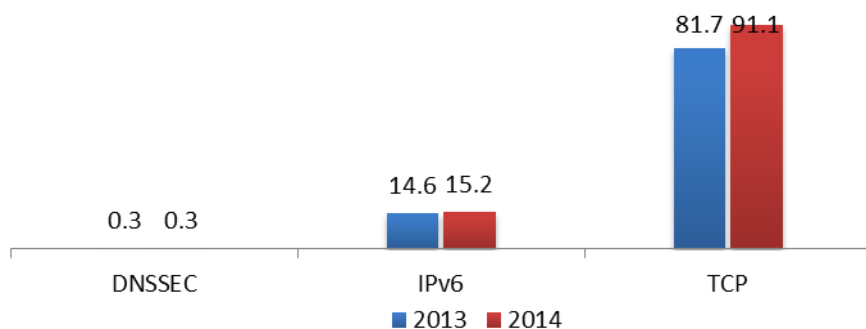


图 10 二级及以下权威域名服务器协议支持比例情况（%）

3.3.4 服务性能

在服务冗余方面，86.5% 的二级及以下权威域具有冗余配置，相比去年有了明显提升（去年该比例为 73.8%），平均每个域所拥有的服务器地址数由去年的 2.0 个增至今年的 3.3 个，具体情况如图 11 所示。

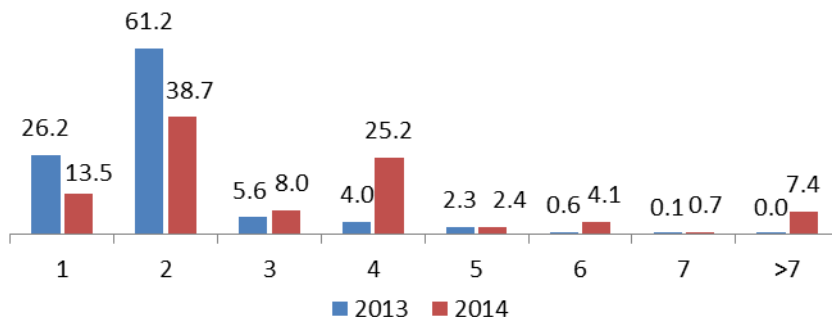


图 11 二级及以下权威域服务地址数量比例分布情况（%）

另外，5.5%的服务器仍然开启了递归服务，相比去年有了显著降低（去年比例为 16.8%），这种配置缺陷具有易遭受 DoS 攻击的风险。

二级及以下权威域名的 TTL 设置分布如图 12 所示。与顶级域名服务器类似，开始有越来越多的二级域选择较大的 TTL 值。

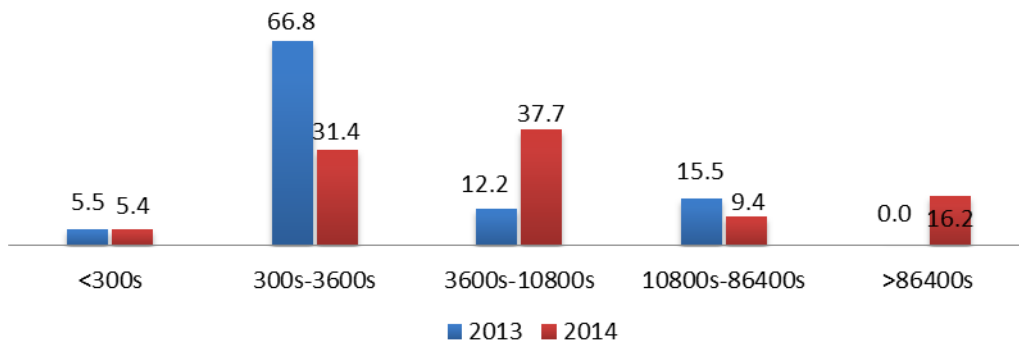


图 12 二级及以下权威域名 TTL 设置分布 (%)

二级及以下权威域名服务器的查询时延分布情况如图 13 所示。可以看出，各服务器的查询时延分布较广、差别巨大。另外，查询时延在 100 毫秒内的服务器比例相比去年有较明显的波动。上述现象一方面反映出各二级及以下权威域名服务器之间服务性能的参差不齐，另一方面也反映出各二级及以下权威域名服务器自身服务性能的非线性，这也是二级及以下权威域名服务器作为数量规模最大的一类域名服务器所表现出的独有特征。

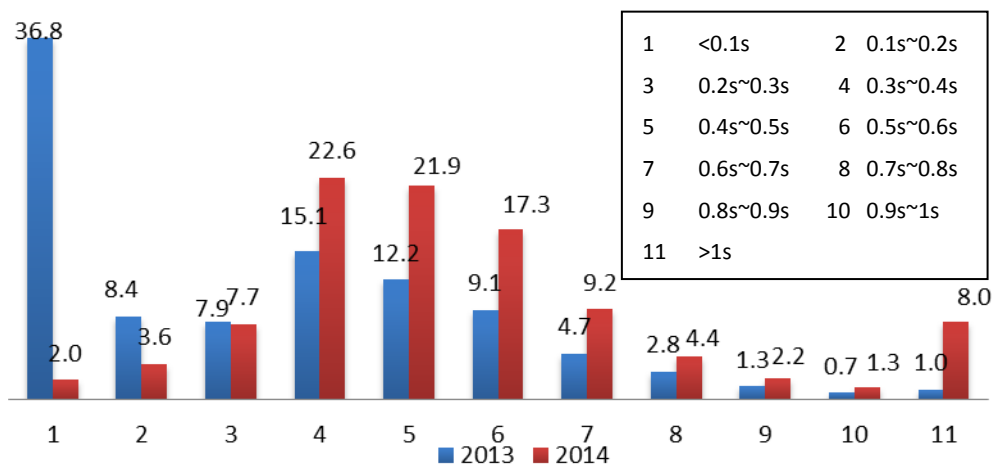


图 13 二级及以下权威域名服务器查询时延比例分布情况 (%)

3.3.5 国内二级及以下权威域名服务系统

3.3.5.1 简介

除了对二级及以下权威域名服务器的监测分析以外，本报告还针对上述服务器中的国内部分做了专门的分析（抽样量级达到 100 万），以下是相关监测数据情况。

3.3.5.2 系统软件

监测显示，国内权威域名服务器采用 Linux 或 Unix 操作系统的比例为 78.3%。DNS 软件中，采用各版本 BIND 软件所占比例为 92.4%（表 3）。但是，仍然有 31.4% 的 BIND 服务器开启了版本应答，存在一定的安全隐患。

表 3 国内二级及以下权威域名服务器 DNS 软件比例分布情况

软件类型	2013年所占比例（%）	2014年所占比例（%）
ISC BIND	92.2	92.4
Unlogic Eagle DNS	3.0	3.2
Microsoft Windows DNS	2.9	2.6
NLnetLabs NSD	0.6	0.6
DJ Bernstein TinyDNS	0.2	0.3
bboy MyDNS	0.2	0.2
JHSOFT simple DNS plus	0.1	0.1
Unlogic Eagle DNS	0.0	0.1
Other	0.8	0.5

3.3.5.3 协议支持

国内权威域名服务器的协议支持情况如图 14、15 所示。

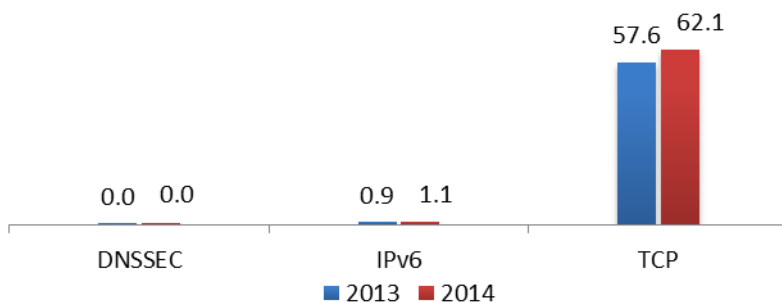


图 14 国内权威域名服务器协议支持情况 (%)

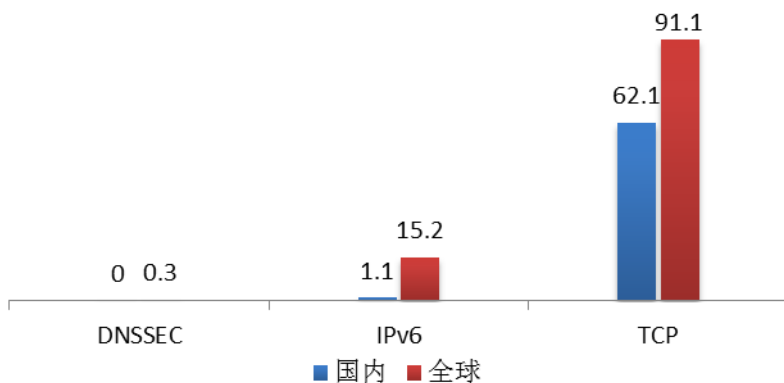


图 15 国内权威域名服务器与全球权威协议支持情况对比 (2014 年) (%)

2014 年国内域名的协议支持情况相对去年略有提升,但还是明显低于全球平均水平。此外,仍然有 23.1%的服务器开启了递归服务,存在遭受 DoS 攻击的风险。

3.3.5.4 服务性能

在服务冗余方面,91.3%的国内二级及以下权威域名具有冗余配置,与去年相比总体冗余程度有了明显提高(图 16~17)。

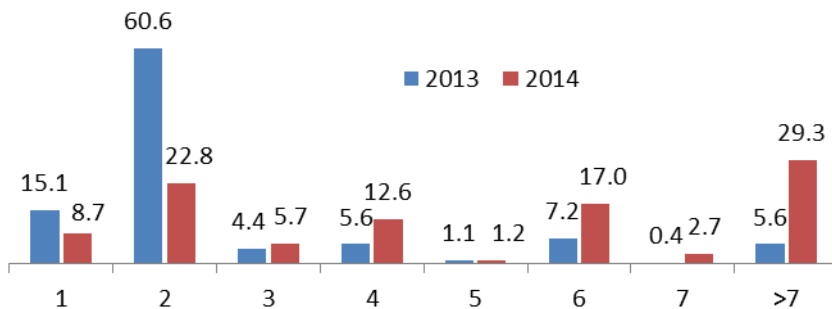


图 16 国内二级及以下权威域服务地址数量比例分布情况 (%)

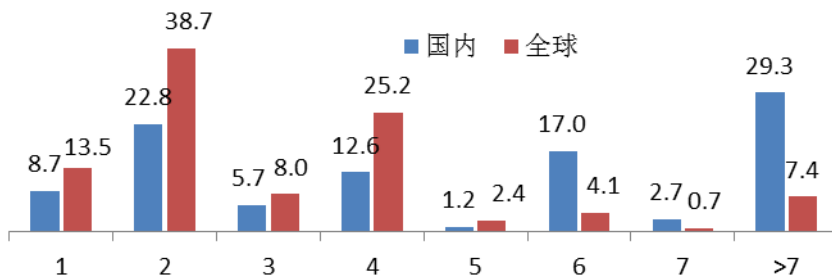


图 17 国内/全球二级及以下权威域名服务器服务地址数量比例分布对比情况 (%)

另外，大约 72% 的国内二级及以下权威域名服务器的解析时延小于 0.5 秒，具有良好的服务性能（图 18）。另外由图 18 可以看出，国内查询时延在 100 毫秒以内的二级及以下权威域名服务器比例明显高于全球水平。

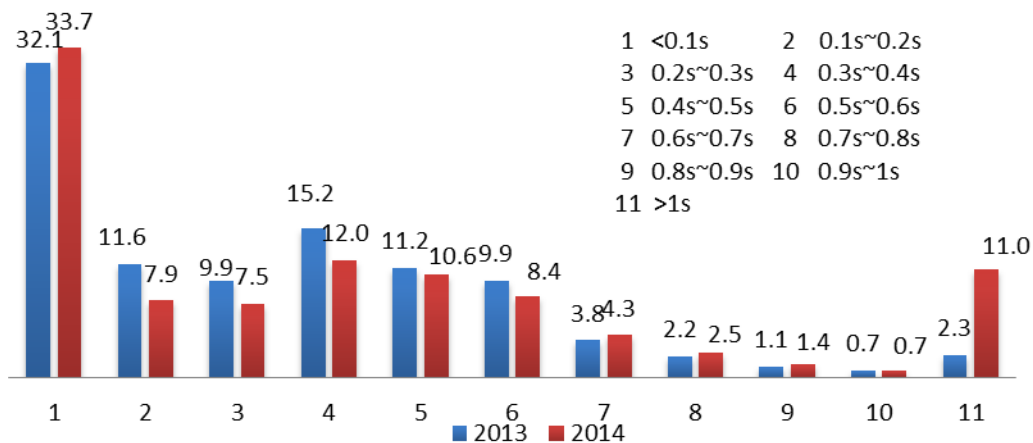


图 18 国内二级及以下权威域名服务器查询时延比例分布情况 (%)

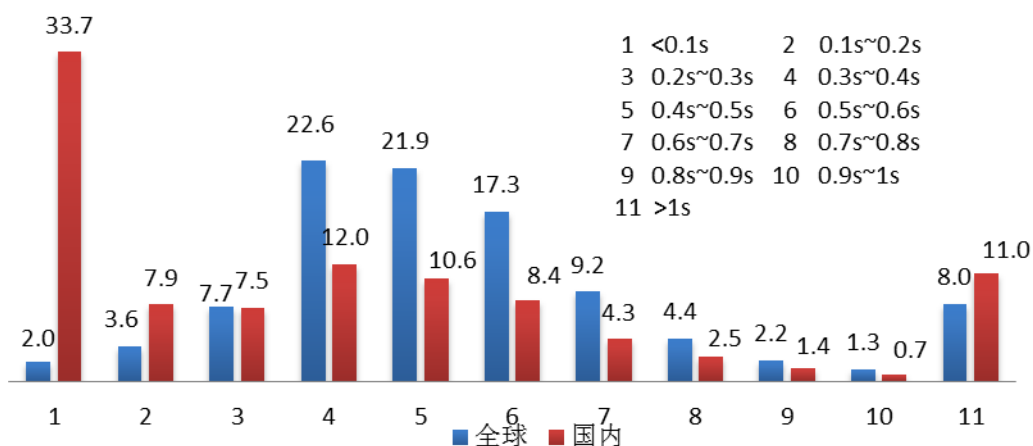


图 19 全球/国内二级及以下权威域名服务器查询时延比例分布对比 (%)

国内二级及以下权威域名的 TTL 设置情况如图 20 所示。大部分国内重点域名的 TTL 设置较大，域名权威数据稳定。

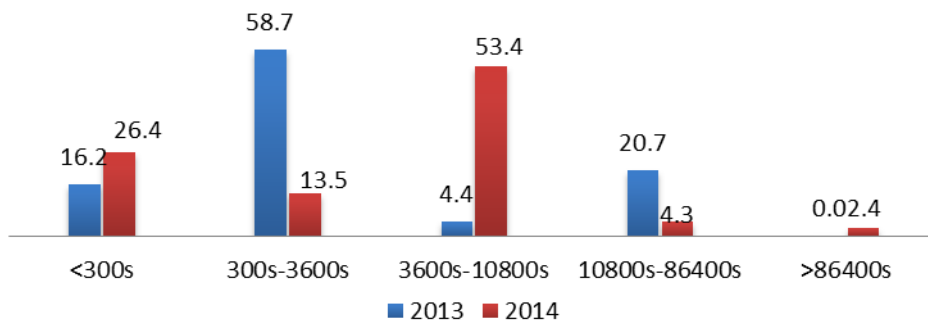


图 20 国内二级及以下权威域名 TTL 设置比例分布情况 (%)

国内二级及以下权威域名与全球权威 TTL 设置情况对比如图 21 所示，与全球相比，国内权威 TTL 小于 300s 的比例较高。

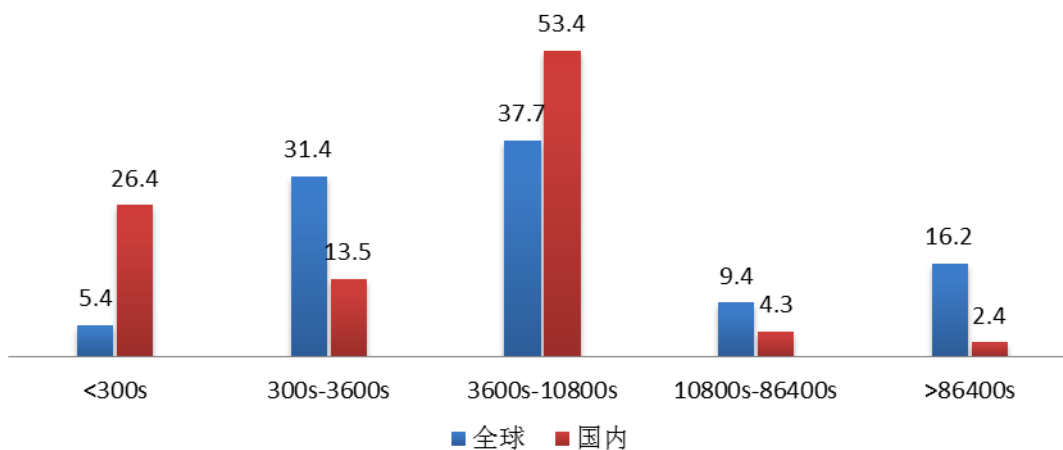


图 21 国内二级及以下权威域名与全球权威 TTL 设置情况对比 (2014 年) (%)

3.3.6 国内重点权威域名服务系统

3.3.6.1 简介

为了能够更加全面深入的了解我国域名体系的整体安全状态，本报告还抽样选择了五百多个来自政府机构、金融机构、网络运营商以及涉及到国计民生行业的热门域名，对其权威域名服务器的安全配置情况进行了监测。

3.3.6.2 系统软件

监测显示，我国重点权威域名服务器采用 Linux 或 Unix 操作系统的比例为 81.4%。DNS 软件中，采用各版本 BIND 软件所占比例为 94.6%（表 4）。但是，

仍然有 17.8% 的 BIND 服务器开启了版本应答，存在一定的安全隐患（去年该比例为 23.2%）。

表 4 国内重点权威域名服务器 DNS 软件比例分布情况

软件类型	2013年所占比例（%）	2014年所占比例（%）
ISC BIND	94.2	94.6
Microsoft Windows DNS	3.5	3.1
NLnetLabs NSD	1.0	1.2
Unlogic Eagle DNS	0.5	0.4
JHSOFT simple DNS plus	0.2	0.2
Cisco CNR	0.2	0.1
Other	0.4	0.4

3.3.6.3 协议支持

国内重点权威域名服务器的协议支持情况如图 22~23 所示。

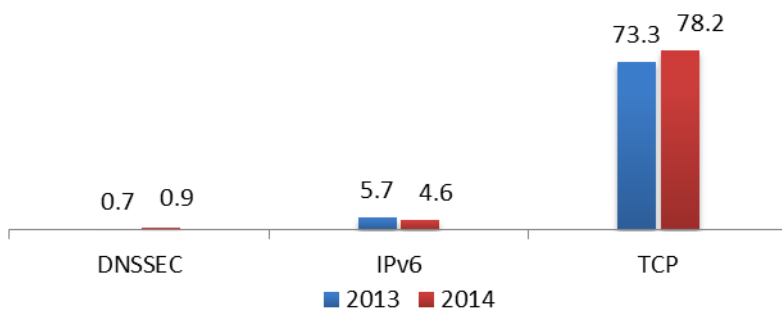


图 22 国内重点权威域名服务器协议支持情况（%）

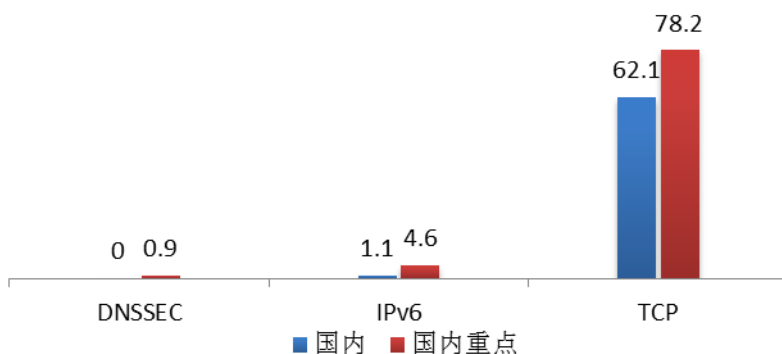


图 23 国内权威域名服务器与国内重点权威协议支持情况对比（2014 年）（%）

与国内域名相比，国内重点域名的协议支持情况相对较好，TCP 支持程度明显较高。此外，仍然有 16.1% 的服务器开启了递归服务，存在遭受 DoS 攻击的风险（去年该数据为 10.2%）。

3.3.6.4 服务性能

在服务冗余方面，92.7%的国内重点权威域名具有冗余配置，总体冗余程度较高（图 24~25）。

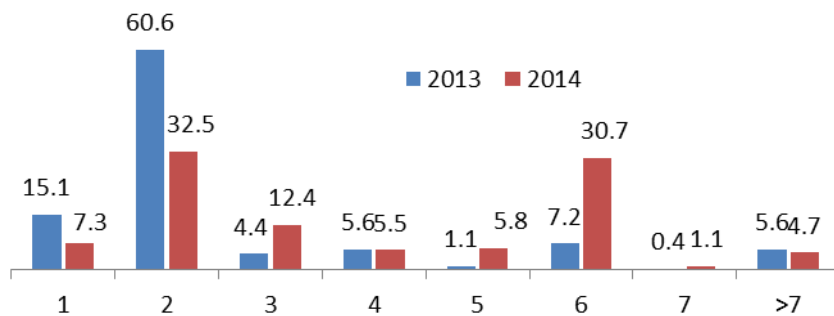


图 24 国内重点权威域名服务地址数量比例分布情况 (%)

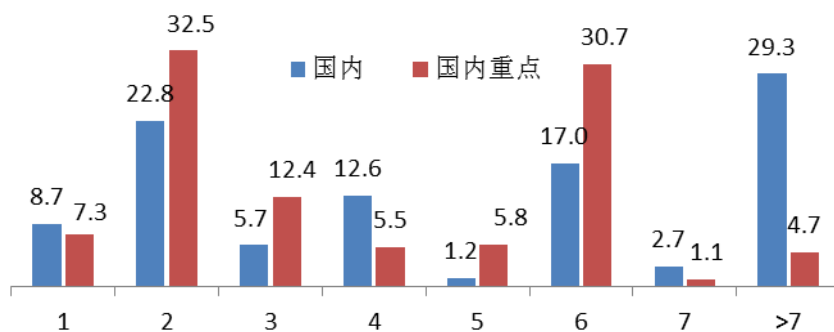


图 25 国内重点权威域名/国内二级及以下权威域名服务地址数量比例分布对比 (%)

国内重点权威域名的 TTL 设置情况如图 26 所示。大部分国内重点权威域名的 TTL 设置较大，域名权威数据稳定。另外，有更高比例的国内重点权威域名将 TTL 设置为特长（大于 86400 秒），如图 27 所示。

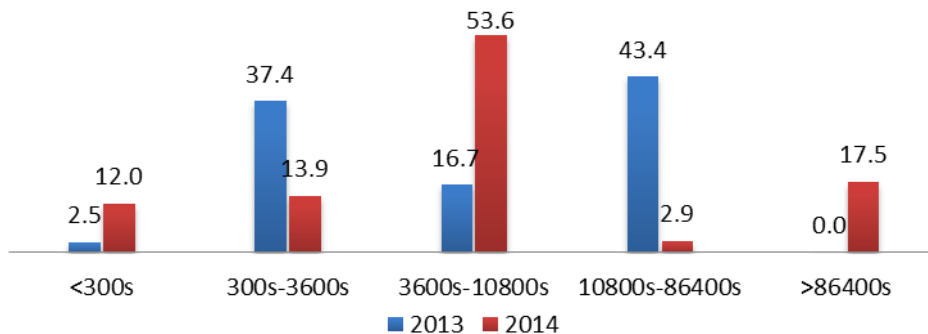


图 26 国内重点权威域名 TTL 设置比例分布情况 (%)

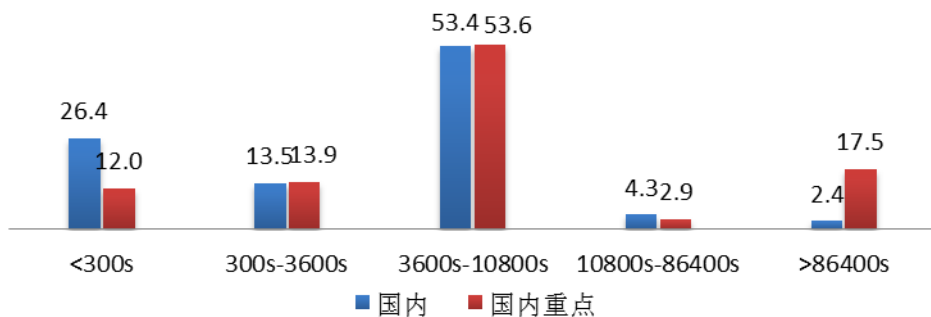


图 27 国内重点域名与国内二级及以下权威域名 TTL 设置情况对比 (2014 年) (%)

此外，大约 96.4% 的国内重点权威域名服务器的解析时延均小于 100 毫秒，与去年相比，整体服务性能明显提升(图 28)。另外从图 29 中也可以看出，国内重点权威域名的整体解析时延明显优于国内平均水平。

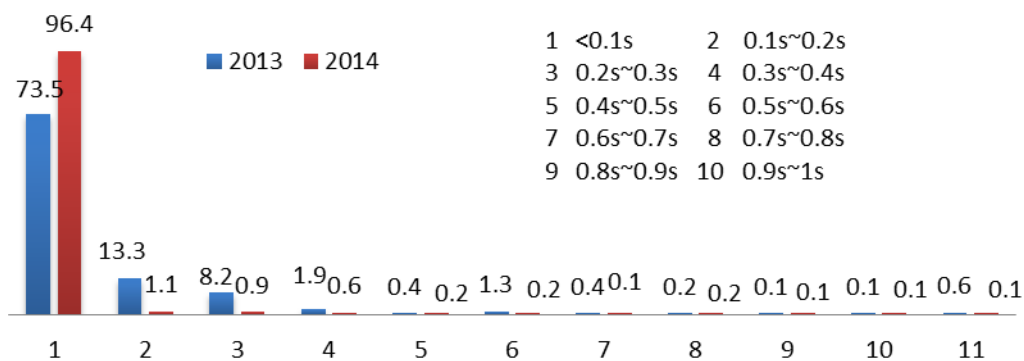


图 28 国内重点权威域名服务器查询时延比例分布情况 (%)

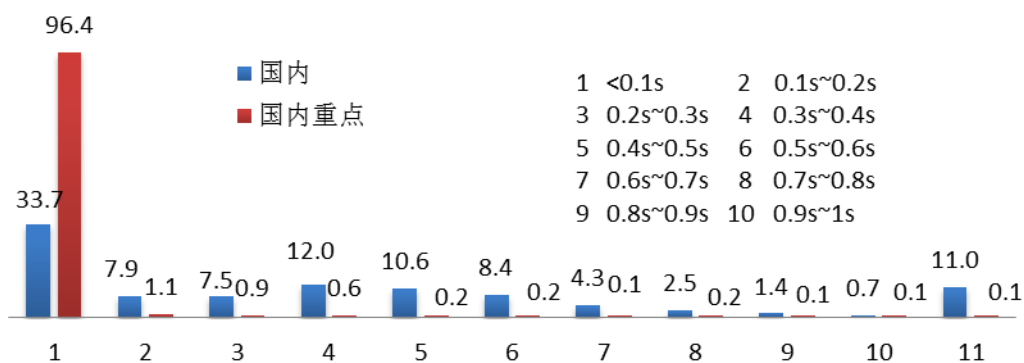


图 29 国内重点权威/国内二级及以下权威域名服务器查询时延比例分布对比 (%)

3.4 递归域名服务系统

3.4.1 简介

递归域名服务系统作为和客户端直接交互的环节，其配置情况和运行状态对于用户所获取到的 DNS 解析数据的完整性、正确性和及时性有直接的影响。为了解全球范围内的递归服务器配置情况和运行状态，本报告以连续七天出现在.CN 顶级域名服务器日志中的递归域名服务器作为样本⁴进行了抽样监测，以下是详细的监测结果。

3.4.2 系统软件

递归域名服务器采用 Linux 或者 Unix 操作系统的比例达到 93.7%。所采用的 DNS 软件中，BIND 所占比例高达 94.4%（表 5）。其中，仍有 34.9% 的 BIND 软件开启了版本应答功能（去年该数据为 38.9%）。

表 5 递归域名服务器 DNS 软件比例分布情况

软件类型	2013年所占比例（%）	2014年所占比例（%）
ISC BIND	96.36	94.43
NLnetLabs NSD	2.07	2.16
Microsoft Windows DNS 2000	0.66	0.69
JHSOFT simple DNS plus	0.35	0.35
Raiden DNSD	0.18	0.16
bboy MyDNS	0.07	0.06
PowerDNS	0.03	0.04
Nominum CNS	0.03	0.04
Microsoft Windows DNS 2003	0.02	0.03
Other	0.23	2.04

3.4.3 协议支持

递归域名服务器的协议支持情况如图 30 所示，与去年监测结果相比，DNSSEC、TCP 的支持情况未出现显著变化。

⁴ 只考虑连续七天日查询量均超过百次的递归服务器，共计约 44.6 万个，抽样 9.5 万个。

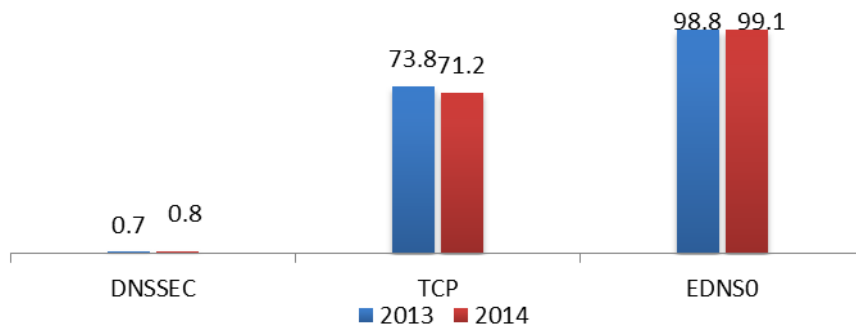


图 30 递归域名服务器协议支持比例情况 (%)

另外，递归域名服务器对于大数据包的支持情况持续改善，支持超过 512 字节的大数据包的比例从去年的 53.9% 进一步增至今年的 98.8%，如图 31 所示。

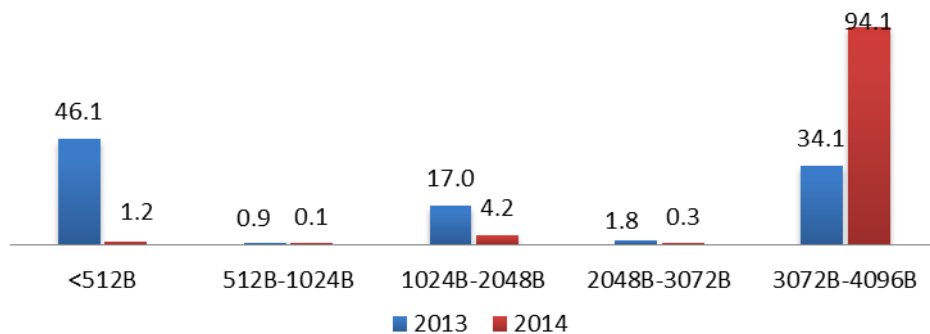


图 31 递归域名服务器最大数据包支持比例分布情况 (%)

长期以来，递归域名服务器一直受到缓存中毒攻击的威胁，而其中主要的原因就是递归域名服务器的端口随机性不足，从而提高了中毒攻击的成功率，图 32 所示为递归域名服务器的端口随机性程度比例分布情况。同去年比较，递归域名服务器的端口随机性程度整体上有所下降。

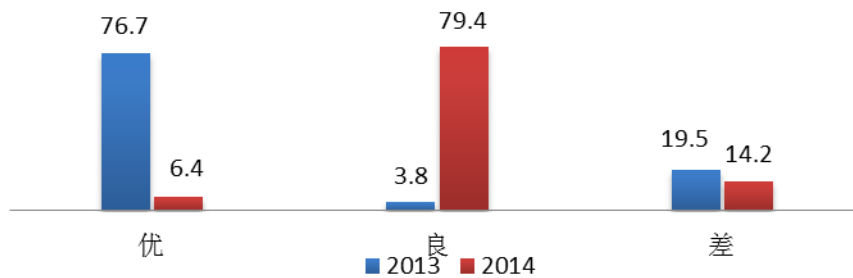


图 32 递归域名服务器端口随机性程度比例分布情况

3.4.4 服务性能

递归域名服务器的查询时延比例分布情况如图 33 所示。递归域名服务器查

询时延比例分布情况与去年的监测结果基本一致，整体上递归域名服务器的查询时延差异较大。

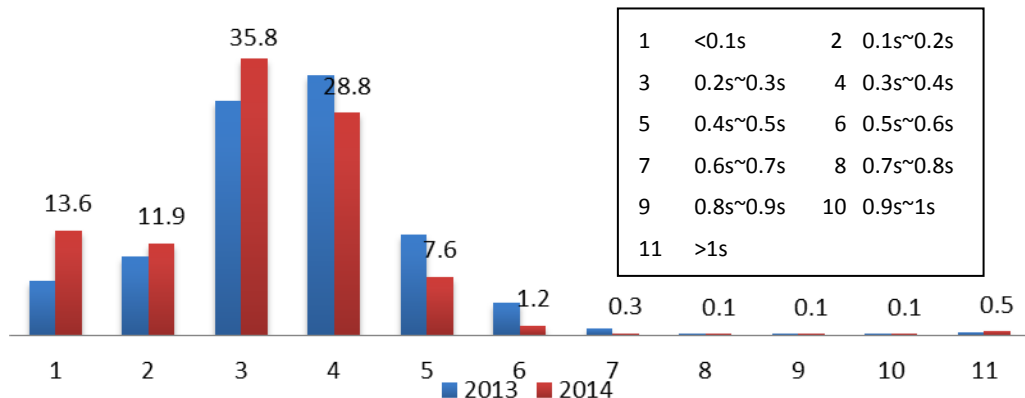


图 33 递归域名服务器查询时延比例分布情况 (%)

3.4.5 国内递归域名服务系统

3.4.5.1 简介

本报告还对位于国内的上述递归域名服务器作了抽取（共计大约 9000 台），并对其进行了针对性的监测。以下是相关监测结果展示。

3.4.5.2 系统软件

结果显示，国内递归域名服务器使用 ISC BIND 软件的比例为 96.3%（表 6），其中 BIND 版本应答比例为 23.0%，略低于全球递归域名服务器的 BIND 版本应答比例（34.9%）。

表 6 国内递归域名服务器 DNS 软件比例分布情况

软件类型	2013年所占比例 (%)	2014年所占比例 (%)
ISC BIND	95.92	96.33
Microsoft Windows DNS 2000	1.71	1.63
Microsoft Windows DNS 2003	1.66	1.72
NLnetLabs NSD	0.26	0.15
Raiden DNSD	0.12	0.06
Paul Rombouts pdnsd	0.04	0.03
bboy MyDNS	0.03	0.03
Unlogic Eagle DNS	0.03	0.03
Other	0.23	0.02

3.4.5.3 协议支持

国内递归域名服务器的协议支持情况如图 34~35 所示。国内递归域名服务器对于 EDNS0 的支持已经非常广泛,但是对于 TCP 支持低于全球平均水平。另外,国内递归域名服务器的 DNSSEC 支持率同样偏低,仅有 1.03%。

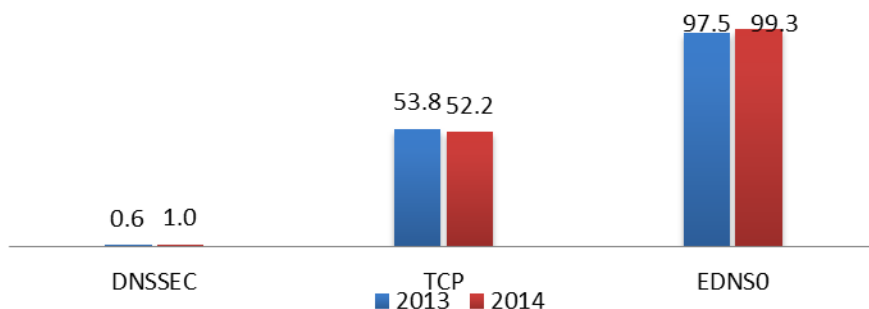


图 34 国内递归域名服务器协议支持比例分布情况 (%)

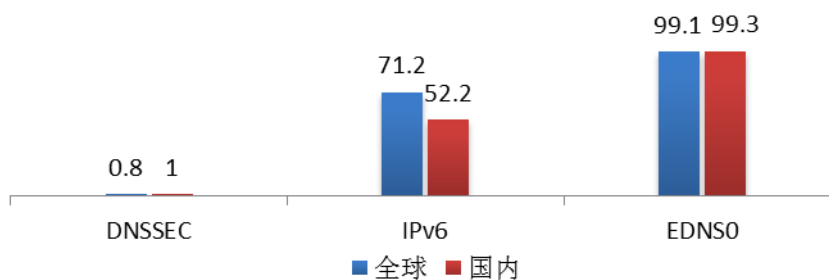


图 35 国内递归域名服务器与全球递归协议支持情况对比 (2014 年) (%)

值得注意的是,国内递归域名服务器对于大数据包的支持情况继续改善,支持超过 512 字节的大数据包的服务器的从去年的 52.5% 进一步增加至今年的 95.5%,具体如图 36 所示。

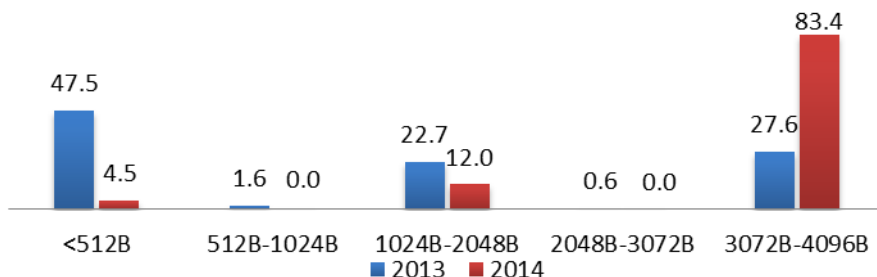


图 36 国内递归域名服务器最大数据包支持比例分布情况 (%)

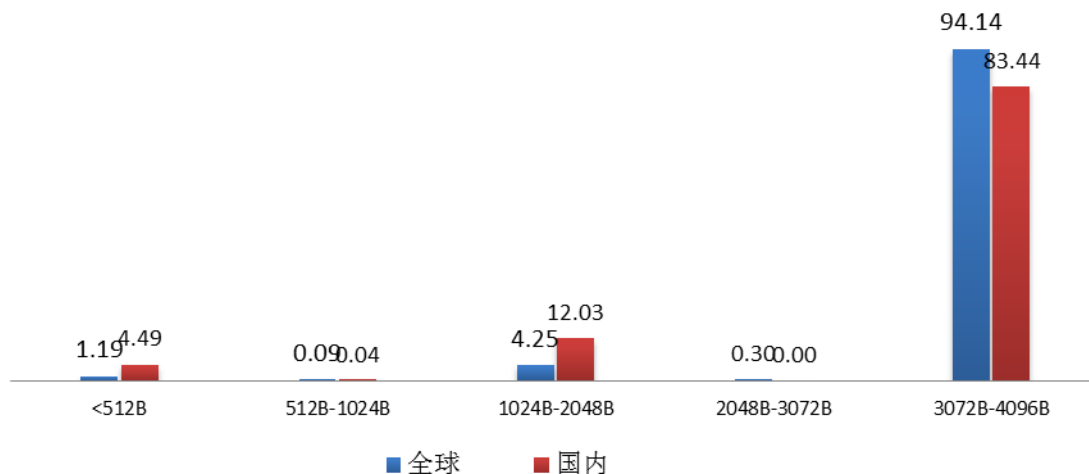


图 37 国内递归域名服务器与全球递归最大数据包支持比例分布对比（2014 年）（%）

国内递归域名服务器的端口随机性程度比例分布情况如图 38 所示，同全球范围内递归域名服务器的端口随机性程度比例分布情况基本一致。

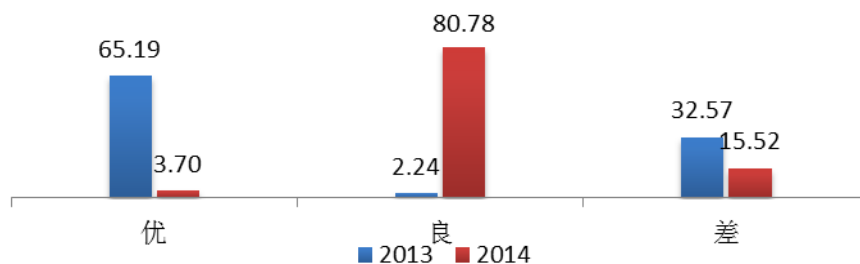


图 38 国内递归域名服务器端口随机性程度比例分布情况

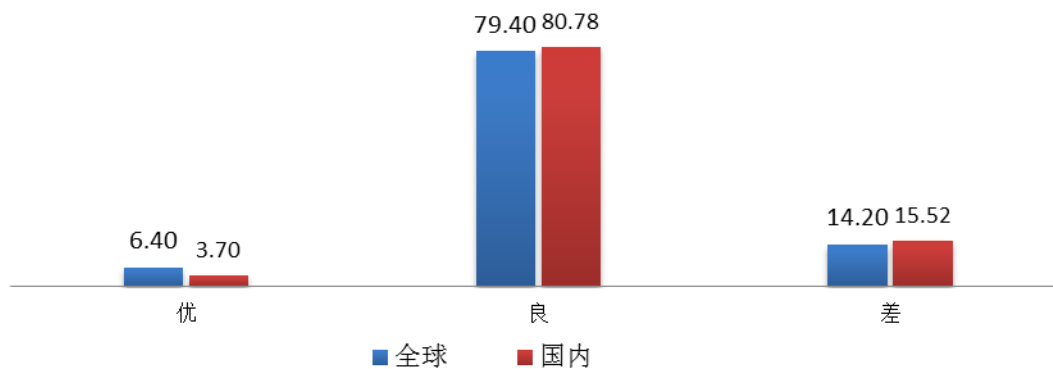


图 39 国内递归域名服务器与全球递归端口随机性程度比例分布对比（2014 年）（%）

3.4.5.4 服务性能

国内递归域名服务器的查询时延分布如图 40~41 所示。国内递归域名服务器查询时延整体情况相比去年有了明显改善，86% 的国内递归域名服务器查询时延集中在 100 毫秒以内，整体解析性能良好。

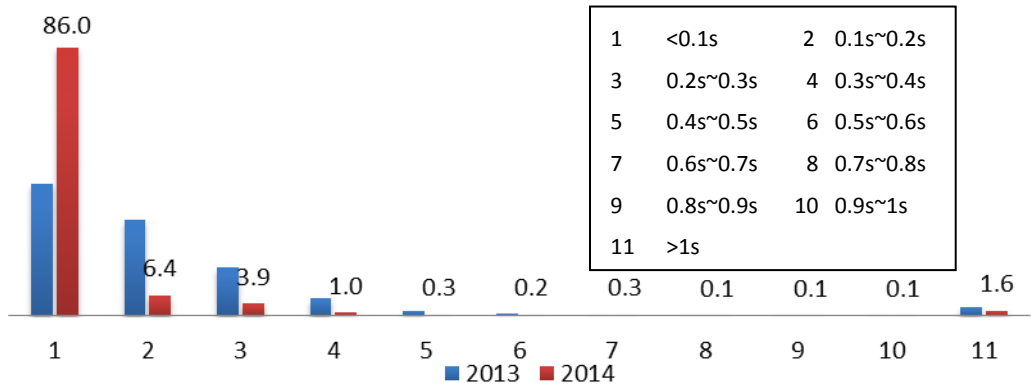


图 40 国内递归域名服务器查询时延比例分布情况 (%)

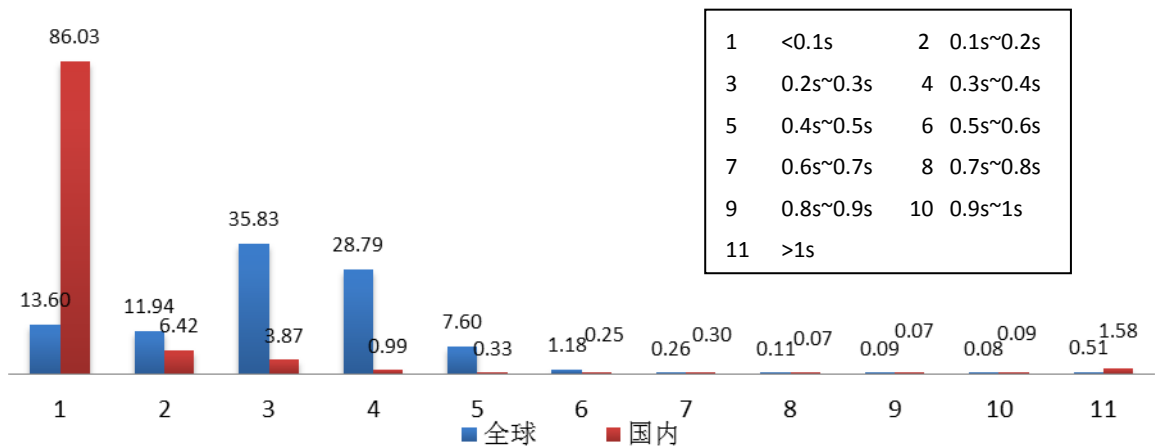


图 41 国内递归域名服务器与全球递归查询时延比例分布对比 (2014 年) (%)

3.4.6 国内主要递归域名服务系统

3.4.6.1 简介

国内基础电信企业所提供的递归域名服务是目前国内互联网用户所使用的主要递归域名服务。另外，一些互联网企业（诸如 114DNS、OpenDNS、Google

等)也面向国内互联网用户提供公共递归服务(Public DNS Service),成为国内递归域名服务的重要组成部分。本报告针对目前国内主要基础电信企业(即中国电信、中国联通、中国移动(含中国铁通))在全国各省份部署的递归域名服务器,以及主流公共递归域名服务器(共计监测近500个对外服务IP地址)进行了探测。

3.4.6.2 系统软件

结果显示,国内主要递归域名服务器使用ISC BIND软件的比例为89.6%(表7),其中BIND版本应答比例为10.1%,低于国内平均水平。

表7 国内主要递归域名服务器DNS软件比例分布情况

软件类型	2013年所占比例(%)	2014年所占比例(%)
ISC BIND	85.46	89.59
Microsoft Windows DNS	6.71	5.14
Vermicelli Totd	4.26	2.14
NLnetLabs NSD	1.62	1.59
Raiden DNSD	1.31	1.16
Paul Rombouts pdnsd	0.14	0.13
Unlogic Eagle DNS	0.06	0.06
Other	0.44	0.19

3.4.6.3 协议支持

如图42~43所示,国内主要递归域名服务器均已实现对EDNS0的支持;对于TCP支持率达到75.8%,高于国内平均水平。另外,国内递归域名服务器的DNSSEC支持率同样偏低,仅有2.2%。

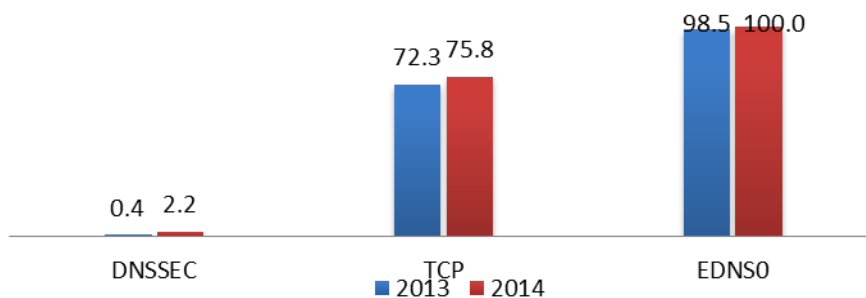


图42 国内主要递归域名服务器协议支持比例分布情况(%)

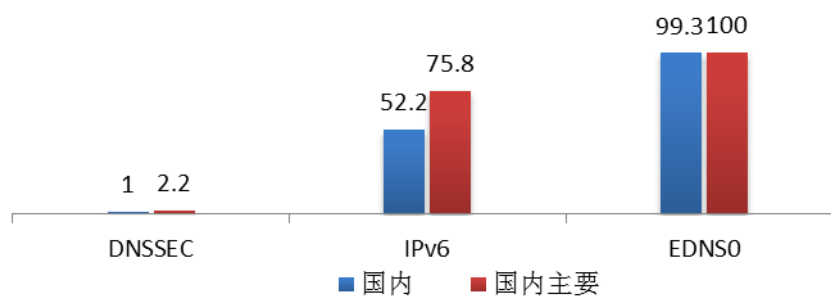


图 43 国内主要递归域名服务器与国内递归协议支持情况对比（2014 年）（%）

国内主要递归域名服务器对于大数据包的支持变化情况同国内整体水平基本保持一致，支持超过 512 字节的大数据包的服务器的比例达到 92.1%（图 44）。

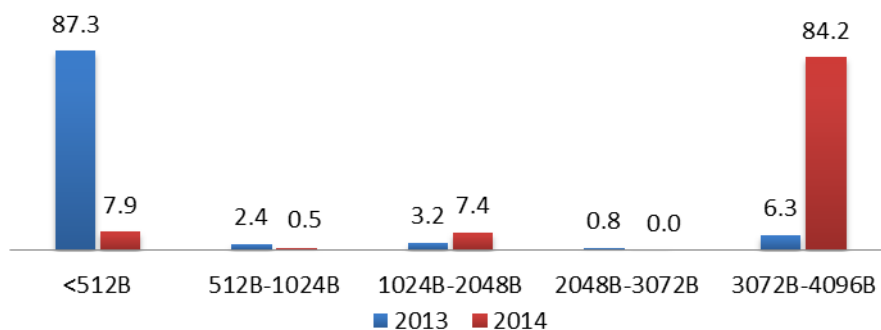


图 44 国内主要递归域名服务器最大数据包支持比例分布情况（%）

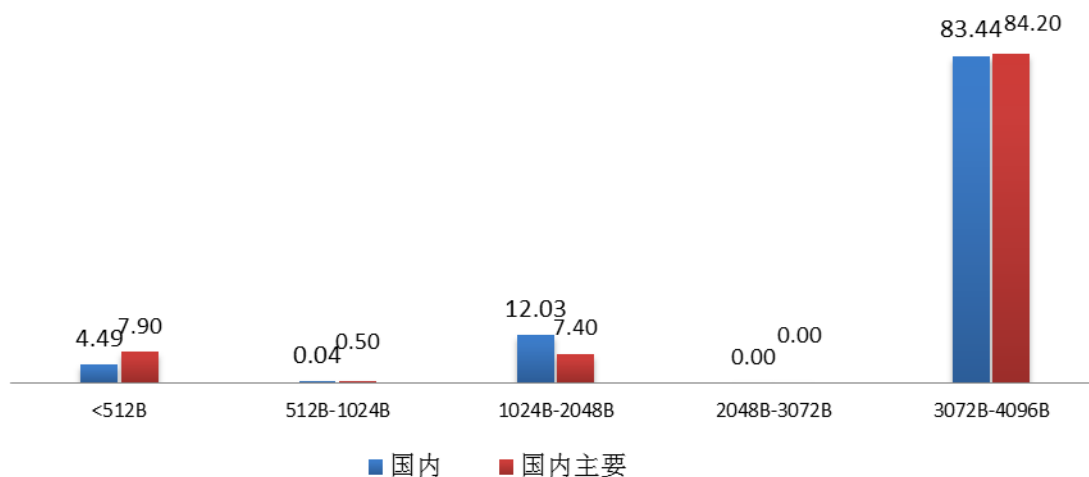


图 45 国内主要递归域名服务器与国内递归最大数据包支持比例分布对比（2014 年）（%）

另外，国内主要递归域名服务器的端口随机性程度整体较高，端口随机性程度为优的服务器的比例达到了 98.2%（图 46）。

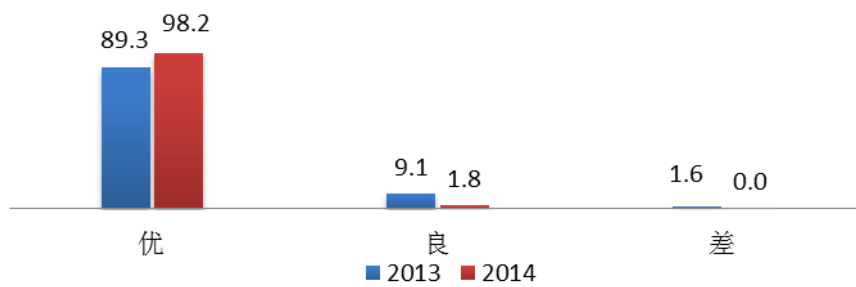


图 46 国内主要递归域名服务器端口随机性程度比例分布情况

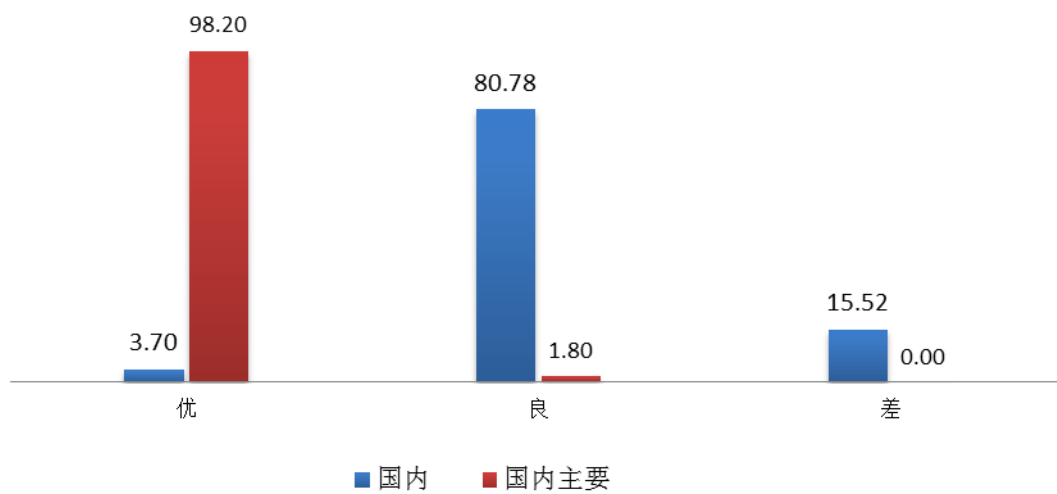


图 47 国内主要递归域名服务器与国内递归端口随机性程度比例分布对比（2014 年）(%)

3.4.6.4 服务性能

如图 48 所示，国内主要递归域名服务器的查询时延分布情况同国内整体水平基本保持一致，92.6%的服务器查询时延集中在 100 毫秒以内，整体解析性能良好。

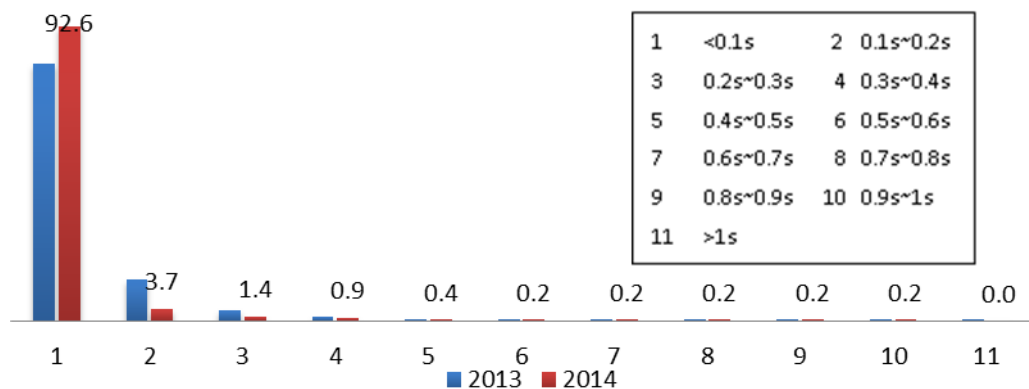


图 48 国内主要递归域名服务器查询时延比例分布情况 (%)

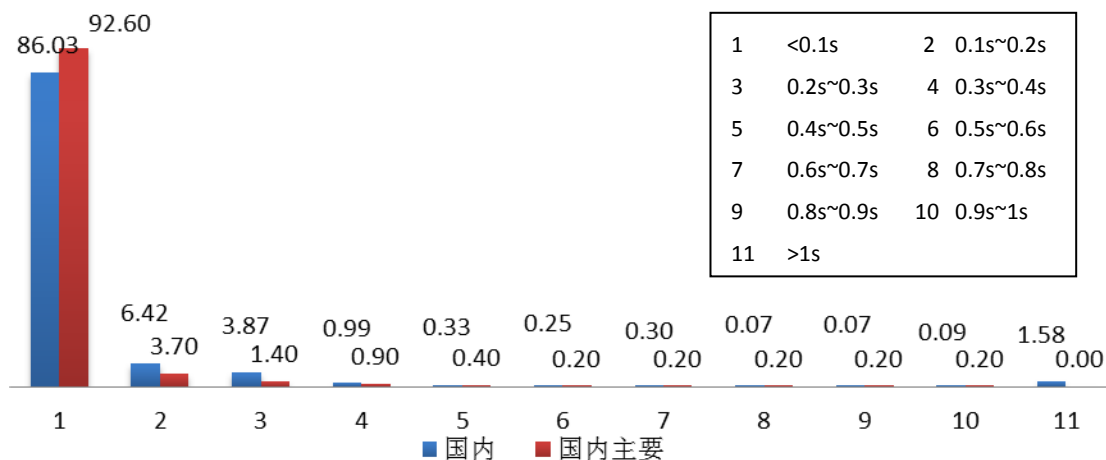


图 49 国内主要递归域名服务器与国内递归查询时延比例分布对比 (2014 年) (%)

4、域名服务安全评估

域名服务体系安全评估旨在针对域名体系各个环节，选择恰当的检测项并进行归一化处理，然后根据域名系统常见安全威胁进行检测项的权重设置，以量化的方式对域名服务体系整体安全状态进行客观、准确的评估。

4.1 权威域名服务系统

权威域名服务器主要用于维护和提供 DNS 权威数据，其可能遭受的攻击包括 DoS 攻击、数据篡改等，对权威服务器的安全评估主要考虑权威系统服务架构、服务器配置、安全功能支持以及服务器性能四个方面。安全指标如表 8 所示。

表 8 权威服务安全指标

安全指标值	含义
$0 \leq \# < 0.4$	服务安全差，如存在配置漏洞
$0.4 \leq \# < 0.7$	服务安全良，如无配置漏洞
$0.7 \leq \# \leq 1$	服务安全优，如具有若干安全防护配置

根据检测结果，全球权威域名服务安全状态分布如图 50 所示。

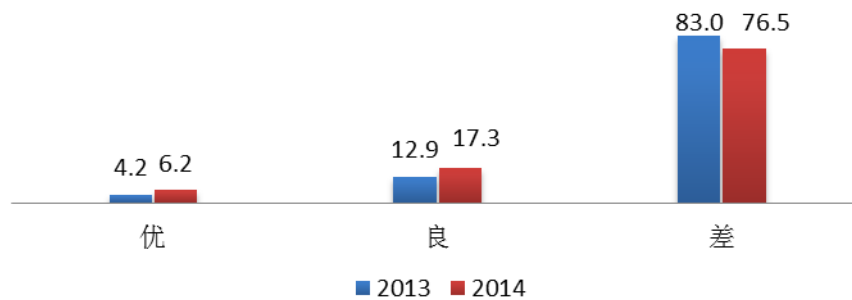


图 50 权威域名服务安全状态分布 (%)

和去年的监测数据相比较，安全状态为差的权威域名服务器比例仍占据 70% 以上，配置漏洞问题在权威域名服务器中普遍存在。另外，安全状态为优的权威域名服务器比例略有提升，由去年的 4.2% 升至今年的 6.2%。

各国家和地区的权威域名服务器平均安全状态如图 51 所示。中国境内的权威域名服务器平均安全指标为 0.40，安全状态为良，与去年值基本持平 (0.406)。

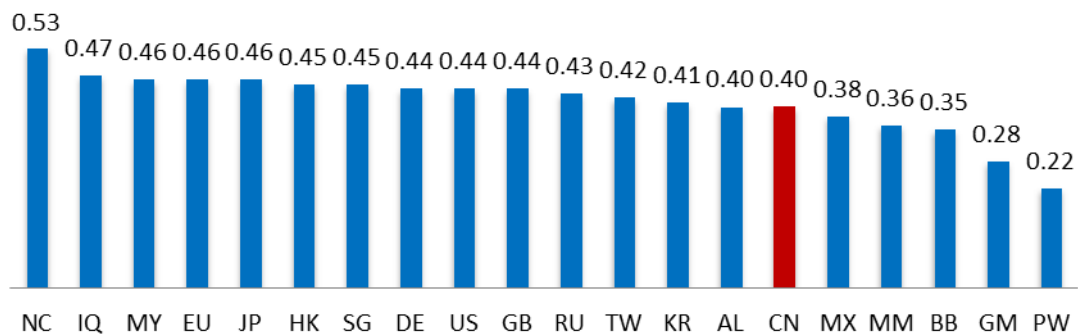


图 51 各国家和地区的权威域名服务平均安全状态分布情况

对于国内重点权威域名服务器，其安全状态分布如图 52 所示。国内重点权威域名服务器的安全状况相对优于全球权威域名服务器的总体安全状况，大部分国内重点权威域名服务器配置较为完善，安全状态良好。

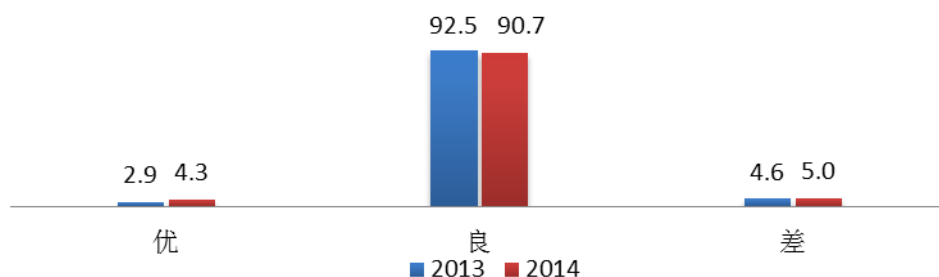


图 52 国内重点权威域名安全状态分布情况 (%)

4.2 递归域名服务系统

递归服务器进行 DNS 解析查询，并对所获取到的权威数据进行缓存，其可能遭受的攻击包括 DoS 攻击、缓存中毒等，对递归服务系统的安全评估主要考虑服务器配置、安全功能支持以及服务器性能三个方面，安全指标如表 9 所示。

表 9 权威服务安全指标

安全指标值	含义
$0 \leq \# < 0.4$	服务安全差，如存在配置漏洞
$0.4 \leq \# < 0.7$	服务安全良，如无配置漏洞
$0.7 \leq \# \leq 1$	服务安全优，如具有若干安全防护配置

根据抽样检测结果，全球递归域名服务安全状态分布如图 53 所示，递归域名服务器安全状态整体较好。

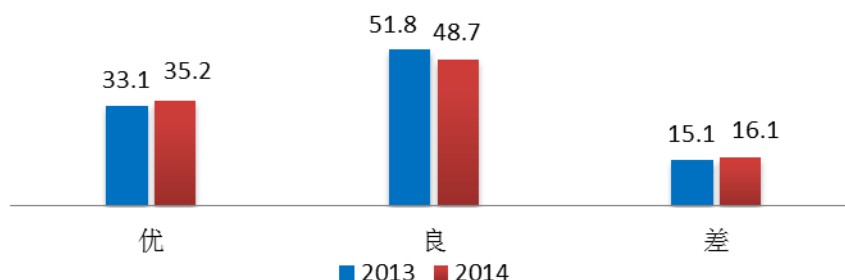


图 53 全球递归域名服务安全状态分布情况 (%)

各国家和地区的递归域名服务器平均安全状态如图 54 所示。中国境内的权威域名服务器平均安全指标为 0.73，相比去年有略微提升（去年为 0.72），安全状态为优。

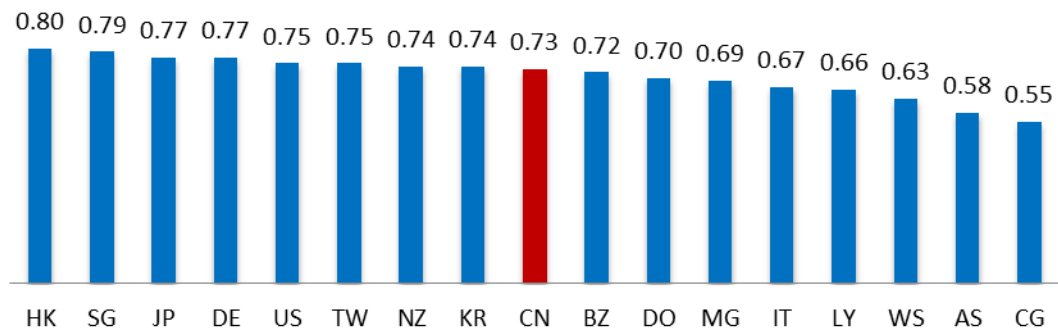


图 54 各国家和地区的递归域名服务平均安全状态分布情况

国内主要递归域名服务器安全状态具体分布如图 55 所示。

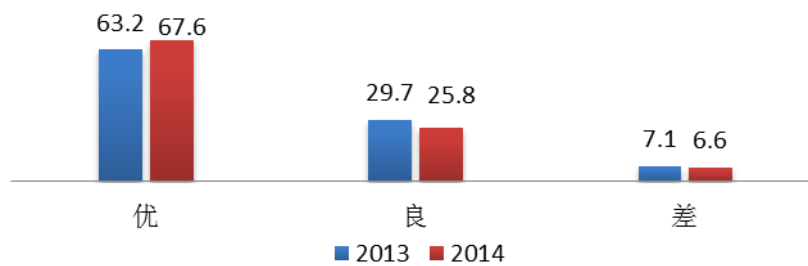


图 55 国内主要递归域名服务安全状态比例分布情况 (%)

国内主要递归域名服务器的安全状况相对优于全球递归域名服务器的总体安全状况，但也有少部分服务器存在一定的安全配置漏洞。

5、我国域名基础设施安全态势分析

基于域名系统的重要性和其在互联网领域牵一发而动全身的地位，对我国域名服务体系进行整体的安全监测和运行分析，不仅可以为国家提供第一手的域名服务系统情况，还可以根据监测分析，向国家提出域名服务系统和网络安全等方面的建议，从而有效地增强国家对互联网的管控能力，从根本上提升我国域名体系的安全保障能力。

本报告的监测结果表明，虽然整体安全状况略有提升，但是我国权威域名服务和递归域名服务在配置管理和运行维护方面仍然存在不同程度的安全隐患。

2014 年我国域名服务体系安全态势呈现出以下几方面特点：

(1) 总体来看，各级域名服务的安全状况同比都有了一定的改善。但除根域名服务以外的其他各级域名服务仍然存在不同程度的安全问题，表现在系统软件、协议支持和服务性能等各个方面。

(2) 虽然 DNSSEC 服务在根区已部署数年，目前在顶级域名服务器中的部署比率也已接近 80%，但在二级及以下权威域名服务器和递归域名服务器中的部署情况仍然步履维艰，这将是今后相当长一段时间内 DNSSEC 部署推进工作的主要着力点。

(3) 今年以来，共计四百多个新通用顶级域开始正式对外服务，未来还将有大批的新通用顶级域涌入，其安全管理将是今后域名安全领域的一项重要内容。

(4) 我国域名服务体系对于 IPv6 协议支持程度整体上进展缓慢，为了有效推动基于 IPv6 的下一代互联网的过渡进程，需要进一步加强域名系统对于 IPv6 资源记录和过渡环境的全面支持。

本报告版权归中国互联网络信息中心（CNNIC）所有。

如引用或转载请注明来源。



国家域名安全联盟

地址：北京中关村南四街四号中国科学院软件园1号楼一层

7*24小时客户服务咨询电话：+86-10-58813000

传真：86-10-58812666

邮政地址：北京349信箱6分箱 CNNIC

邮政编码：100190

网址：<http://www.cnnic.cn>

<http://中国互联网络信息中心.中国>

电子邮件：ndsa_public@cnnic.cn