ICS 35.100.70
L 79

YD

中华人民共和国通信行业标准

YD/T 2091-2010

公共域名解析系统安全要求

Security specification for public DNS resolution system

2010-12-29 发布　　2011-01-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本标准是“域名系统运行技术规范体系”系列标准之一，该系列标准包括：

——《域名系统运行总体技术要求》

——《域名系统权威服务器运行技术要求》

——《域名系统递归服务器运行技术要求》

——《IPv6 网络域名服务技术要求》

——《公共域名解析系统安全要求》

——《域名服务安全框架技术要求》

——《域名系统授权体系技术要求》

——《域名系统安全防护要求》

——《域名系统安全防护检测要求》

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国互联网络信息中心、国家计算机网络应急技术处理协调中心。

本标准主要起草人：毛　伟、李晓东、王　伟、金　键、沈　烁、胡安磊。

公共域名解析系统安全要求

1 范围

本标准规定了公共域名解析系统的安全方针、技术要求以及管理要求。

本标准适用于为互联网公众提供域名解析服务的国内各级单位，适用对象包括根域名解析系统，顶级域名解析系统，其他各级域名解析系统、递归域名解析系统。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YD/T 2136-2010　域名系统授权体系技术要求

YD/T 2137-2010　域名系统递归服务器运行技术要求

YD/T 2138-2010　域名系统权威服务器运行技术要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

域名　Domain Name

域名系统名字空间中，从当前节点到根节点的路径上所有节点标记的点分顺序连接，如图1中对应的域名“www.bj.cn.”。

在本标准中，域名的范围包含了由数字、英文字母及连接符（“-”）等ASCII编码组成的英文域名，以及由非ASCII编码的字符组成的国际化域名（IDN）两大范畴，比如.中国，.网络，.公司等。

3.1.2

域　Domain

域名系统名字空间中的一个子集，也就是树形结构名字空间中的一棵子树。这个子树根节点的域名就是该域的名字，如图1中灰色圆圈所示的域“net.cn”。

3.1.3

顶级域　Top Level Domain

域名系统名字空间中根节点下最顶层的域。顶级域分为国家及地区代码顶级域（Country Code Top Level Domain, ccTLD）、通用类别顶级域（Generic Top Level Domain, gTLD）和行业类别顶级域（sponsored Top Level Domain，sTLD）等三种不同类型。如图1中 “cn”为中国顶级域，“com”、“net”、“arpa”均为通用类别顶级域，而“tel”、“mobi”则是行业类别顶级域。

3.1.4

资源记录 Resource Record

在域名系统中用于存储与域名相关的属性信息，简称RR。每个域名对应的记录可能为空或者多条。

域名的资源记录由名字（Name）、类型（Type）、种类（Class）、生存时间（TTL）、记录数据长度（Rdlength）、记录数据（Rdata）等字段组成。

3.1.5

域名系统 Domain Name System

一种将域名映射为某些预定义类型资源记录（Resource Record）的分布式互联网服务系统，网络中域名解析系统间通过相互协作，实现将域名最终解析到相应的资源记录。

域名系统由名字空间和资源记录、域名解析系统、解析器三部分共同组成。域名系统的名字空间是一个分层次的（Hierachical）树状结构，在资源记录中存储了包含IP地址等与域名相关的多种信息，通过不同层次上域名解析系统的协作实现对域名属性信息的分布式检索。

3.1.6

域名解析系统 Domain Name Service System

提供域名解析服务的系统，由权威域名解析系统、递归域名解析系统组成。

3.1.7

权威域名解析系统 Authoritative Domain Name Service System

对于某个或者多个区具有权威的服务系统，权威解析服务系统保存着其所拥有权威的区的原始域名资源记录信息。根据域名系统名字空间的树状结构，权威域名解析系统包括根域名解析系统、顶级域名解析系统和其他各级域名解析系统。

3.1.8

递归域名解析系统 Recursive Domain Name Service System

负责接收用户（解析器）的解析请求，并通过查询本地缓存或者执行从根域名解析系统到被查询域名所属权威服务系统的递归查询过程，获得解析结果并返回给用户的域名解析系统。

一般来说，按照职能的不同，域名解析服务系统本身可以分为权威解析服务系统和本地（递归）解析服务系统两类。这两者之间最大的区别就是，权威解析服务系统通常不提供递归解析（Recursive Resolution）服务，它只负责维护和保存它所拥有权威的域的资源记录信息,并且接受递归解析服务系统的查询请求；而本地（递归）解析服务系统则通常不会维护或者管理任何域的资源记录数据，它只负责接收用户（解析器）的查询，并且通过本地缓存或者向包括根在内的权威名字服务系统发出查询从而获得查询结果。

3.1.9

区文件 Zone File

某个区内的域名和资源记录及相关的权威起始信息（Start of Authority，SOA）按照一定的格式进行组合，从而构成存储这些信息的区文件。其中，权威起始信息包含了区的管理员电子邮件地址（Mail Address）、序列号（Serial）、更新周期（Refresh）、重试周期（Retry）和过期时间（Expire）等信息。

3.1.10

主域名解析系统 Master Domain Name Service System

被配置成区数据发布源的权威域名解析系统。

3.1.11

辅域名解析系统 Slave Domain Name Service System

通过区传送协议来获取区数据的权威域名解析系统。

3.1.12

区传送 Zone Transfer

将区的资源记录内容从主服务系统向辅服务系统传送的过程，用于实现主、辅服务系统间的数据同步。

3.1.13

解析器 Resolver

向名字服务系统发送域名解析请求，并且从名字服务系统返回的响应消息中提取所需信息的程序。解析器软件通常集成到操作系统内核或者应用软件中。

3.2 缩略语

下列缩略语适用于本标准。

ccTLD	Country Code Top Level Domain	国家码类别顶级域
DNS	Domain Name System	域名系统
gTLD	Generic Top Level Domain	通用类别顶级域
IP	Internet Protocol	网际协议
KSK	Key Signing Key	密钥签名密钥
RFC	Request For Comments	请求注解
SOA	Start of Authority	起始授权
TCP	Transmission Control Protocol	传输控制协议
TTL	Time to Live	生存时间
TLD	Top Level Domain	顶级域
UDP	User Datagram Protocol	用户数据报协议
ZSK	Zone Signing Key	区签名密钥

4 概述

域名解析服务是一种互联网应用层资源的寻址服务，是其他互联网络应用服务的基础。常见的互联网络应用服务有Web服务，电子邮件服务，FTP服务等，它们都是以域名服务为基础，来实现系统内部资源的寻址和定位的。

域名解析系统是以树型拓扑结构来定义的，由不同类别的域名解析系统服务机构负责不同级域名的解析服务。其对应关系如图1所示。

树的顶层是根域的服务器（Root），目前一共有13个根服务器遍布全球。逻辑上每一个根服务器对外都为不同的IP地址，物理上每一个IP地址标识的根服务器则是通过任播（Anycast）技术，由若干台物理服务器构成。接下来一层为顶级域（TLD）层，由国家及地区代码顶级域（ccTLD）、通用类别顶级域（gTLD）和行业类别顶级域（sTLD）三类组成。域名树型拓扑结构中顶级域下层的二级域、三级域，以及再下一层子域域名的解析服务，如“.com.cn”、“.org.cn”、“.bj.cn”等，通常是由获得授权的权威名字服务器来完成。

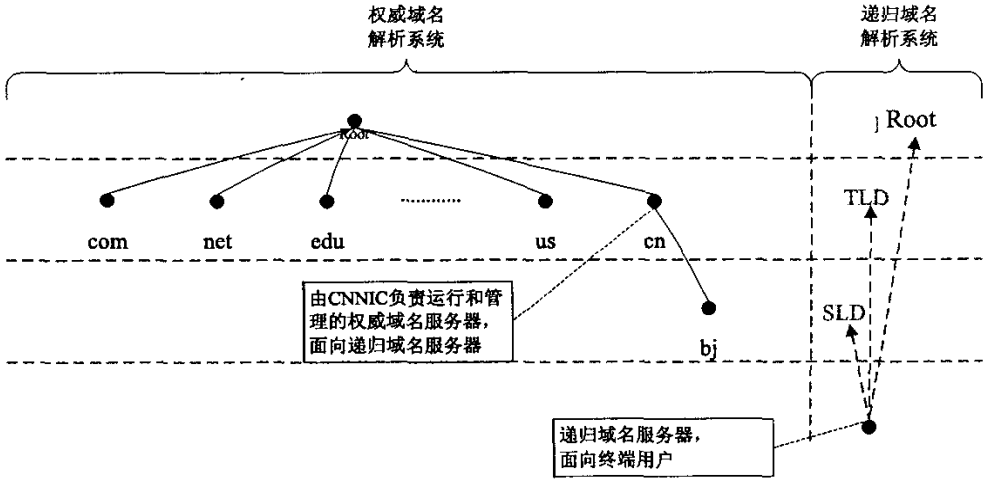

图1 全球域名服务体系结构图

整个域名解析系统从职能上看，包括两大类系统，即权威域名解析系统（Authoritative DNS）和递归域名解析服务（Recursive DNS）。权威域名系统服务是指拥有某个区的域名信息，并为该区提供域名解析的服务。权威域名系统通常面向的不是终端用户。图1中，cn和bj.cn的域名解析系统就属于权威域名系统。递归域名系统则相反，它不针对某个区提供域名解析服务，而是直接面向终端用户，为终端用户提供递归的域名解析系统。

针对上述域名解析系统的组成结构，本标准应涵盖权威域名解析系统、权威域名服务器、递归域名解析系统以及递归域名服务器等方面的安全要求。

5 公共域名解析系统安全方针

公共域名解析系统管理者应根据业务目标制定清晰的安全指导方针，并通过在整个域名解析服务系统运行单位内颁布和维护安全方针文件来表明对公共域名解析系统安全的支持和承诺。

5.1 公共域名解析系统安全方针文件

安全方针文件应说明运行管理承诺，并提出在公共域名解析系统安全管理方面的方法。文件中包括以下内容：

a） 公共域名解析系统的技术要求，包括但不限于：

1） 权威域名解析系统技术要求；

2） 递归域名解析系统的技术要求；

3） 授权安全要求；

4） DNS数据备份要求。

b） 公共域名解析系统的管理要求，包括：

1） 资产管理要求；

2） 人员管理要求；

3） 运行管理要求；

4） 物理和环境安全要求；

5） 设备安全要求；

6） 通信和操作安全要求；

7） 访问控制要求；

8） 连续性管理要求。

5.2 安全方针文件的评审

按计划的时间间隔或当重大变化发生时进行安全方针的评审，确保它持续的适用性、充分性和有效性。尤其当相关的域名系统运行、技术、安全等方面的标准变更之后。

6 技术要求

6.1 权威域名解析系统技术要求

6.1.1 功能和协议要求

作为权威域名系统的权威服务器，应具备权威服务器的基本功能，即能够正常处理来自互联网络的任何客户端的域名查询请求，和该区的可信任辅服务器之间实现安全的区数据传送，支持DNS安全协议。其实现必须符合IETF相关RFC标准，符合必备的接口和安全协议，完整的安全要求和要求支持的RFC列表见《域名系统权威服务器运行技术要求》。

6.1.2 拓扑规划要求

针对某个权威域，提供权威域解析的服务器数量应保证多台备份，提供权威域解析的服务器应部署在多个不同的自治域网络中，并且建议在地理上进行合理分配分布，达到抗自然灾害等灾备目的。具体部署数量和分配要求见《域名系统权威服务器运行技术要求》。

6.1.3 性能要求

权威域名解析系统应保证业务处理能力，预留应对突发流量的处理能力，满足《域名系统权威服务器运行技术要求》中规定的解析性能要求以及域名数据同步要求。

6.1.4 权威域名服务器安全要求

权威服务器的安全决定了权威服务的可靠性和稳定性，是整个域名解析系统安全的核心问题。权威域名解析系统需要保证DNS服务的的数据安全、解析安全以及传输安全，具体要求见《域名系统权威服务器运行技术要求》。

6.2 递归域名解析系统技术要求

递归服务器是最终面对互联网用户的域名服务器，对于保障各种互联网应用的正常运行具有重要意义。此外，针对递归服务器的各类攻击（缓存中毒、域名劫持、DNS 放大攻击等）日益威胁互联网系统的安全。因此，有必要对互联网中递归服务器的构建进行规范化。

6.2.1 协议要求

作为递归域名系统的递归服务器，应具备递归服务器的基本功能，即能够安全的实现查询，缓存等功能。其实现必须符合IETF相关RFC标准，符合必备的接口和安全协议，完整的安全要求和要求支持的RFC列表具体要求见《域名系统递归服务器运行技术要求》。

6.2.2 拓扑规划要求

针对某个自治域内，提供递归域解析的服务器数量应保证多台备份。同一自治域内的不同递归服务器在部署上应该进行分布，同一用户访问两台服务器的路径上不存在单一故障点。具体部署数量和要求见《域名系统递归服务器运行技术要求》。

6.2.3 性能要求

递归域名解析系统应保证业务处理能力，预留应对突发流量的处理能力，满足《域名系统递归服务器运行技术要求》中规定的解析性能要求以及域名数据同步要求。

6.2.4 递归域名服务器安全要求

递归服务器的安全决定了其服务域内域名服务的可靠性和稳定性，是局部范围内域名解析系统安全的核心问题。递归服务器应该保证安全远程管理和安全缓存清空等数据安全；保证解析软件和同步等解析安全，具体要求见《域名系统递归服务器运行技术要求》。

6.2.5 中文域名支持要求

中国境内的递归服务器应配置对中文域名（CDN/IDN）的支持，比如.中国，.中國，.网络，.公司，.網絡，公益，.政务。

递归服务器的配置应确保通过其进行查询的用户能够正确解析相应的域名。

6.3 授权安全要求

公共域名解析系统应符合《域名系统授权体系技术要求》。

6.4 DNS 数据备份要求

6.4.1 日志存放形式

域名解析日志应完全保存，并以冷备份的方式按日期存放。冷备份的方式应有两种以上，包括硬盘、磁带、光盘等方式。

热备份是将日志存放在服务器的存储设备上。

6.4.2 日志存放时间

冷备份应保留最新的3个月的日志。并建议进行永久保留。

热备份的保留时间，应以满足域名管理者的日志分析需求为标准。

6.4.3 日志分析

应建立解析服务日志的分析制度，以便于及时发现服务中的异常情况，并对非法访问采取必要的防范措施。

7 管理要求

7.1 资产管理要求

7.1.1 资产清单

应清晰的识别公共域名解析系统所涉及的资产，编制并维护公共域名解析系统的核心资产清单。清单中应包括所有为从灾难中恢复而需要的资产，与公共域名解析系统相关的资产可能包括：信息资产、软件资产、物理资产、服务、人员、无形资产等。

7.1.2 资产责任人

与公共域名解析系统有关的所有信息和资产都应指定部门和人员承担责任，资产责任人应确保：

a） 与公共域名解析系统相关的信息和资产进行了适当的分类；

b） 确定并周期性审查访问限制和分类。

7.1.3 资产的合规使用

与公共域名解析系统相关的信息和资产使用规则应当确认并形成文件加以实施。

7.1.4 以资产清单为基础的脆弱性和威胁分析

a） 从技术脆弱性和管理脆弱性两个方面，对公共域名解析系统进行脆弱性的分析；

b） 从技术威胁、环境威胁、人为威胁3个方面，对公共域名解析系统进行威胁分析。

7.2 人员管理要求

在公共域名解析系统的管理人员和第三方人员的整个任职周期内，包括聘任前、聘任中、离职3个阶段，采取相应的控制措施，降低公共域名解析系统所面临的人为威胁。应考虑：

a） 确保公共域名解析系统管理人员和第三方人员理解其职责，确保其具备相应的技术能力，以降低公共域名解析系统被破坏或者不当使用的风险；

b） 应对公共域名解析系统管理人员和第三方人员提供适当程度的安全意识和安全技术培训以及公共域名解析系统相关信息和资产的正确使用方法，并建立一个正式的处理安全违规的纪律处理过程。

c） 应有流程或规定规范公共域名解析系统管理人员和第三方人员退出公共域名解析系统的管理，并确保相关人员归还所有设备及删除他们的对公共域名解析系统的所有访问权限。

7.3 运行管理要求

公共域名解析系统应遵守《域名系统权威服务器运行技术要求》以及《域名系统递归服务器运行技术要求》中相关的运行管理要求。

此外，公共域名解析系统中所有涉及到的服务应对国家主管部门提供数据采集接口，并应按照国家主管部门《互联网网络安全信息通报实施办法》的规定对相应网络安全事件进行通报。

7.4 物理和环境管理要求

7.4.1 设置安全的区域

a） 应设置安全边界（诸如墙、卡控制的入口或有人管理的接待台等屏障）来保护公共域名解析系统信息和资产所在的区域；

b） 应设置恰当的进出控制措施，确保只有授权任用才能进出，同时进出的信息要予以记录和审计；

c） 应有适当的措施来避免火灾、洪水、地震、爆炸、社会动荡和其他形式的自然灾难或人为灾难对域名解析系统所在区域的破坏；

d） 应有足够的支持性设施（例如电、供水、排污、加热/通风和空调）来支持域名解析系统。支持性设施应定期检查并适当的测试以确保它们的功能，减少由于它们的故障或失效带来的风险。

7.5 设备管理要求

7.5.1 设备安置和保护

a） 公共域名解析系统的设备应进行适当安置，以防止对相关设备的未授权物理访问；

b） 应采取控制措施以减小潜在的物理威胁的风险，例如偷窃、火灾、爆炸、烟雾、水（或供水故障）、尘埃、震动、化学影响、电源干扰、通信干扰、电磁辐射和故意破坏；

c） 对于可能对公共域名解析系统运行状态产生负面影响的环境条件（例如温度和湿度）要予以监视；

d） 建筑物应采用避雷保护，所有进入的电源和通信线路都应装配雷电保护过滤器；

7.5.2 布线和设备维护

a） 应保证传输数据或支持信息服务的电源布缆和通信布缆免受窃听或损坏；

b） 使用文件化配线列表减少失误的可能性；

c） 要按照供应商推荐的服务时间间隔和规范由已授权人员对设备进行维护，同时保存所有可疑的或实际的故障以及所有预防和纠正维护的记录；

d） 应绘制与当前运行情况相符的系统拓扑结构图。

7.5.3 设备的安全检测和监控

a） 公共域名解析系统的硬件设备应进行安全检测，确保其满足相应的行业标准、技术规范等，并保留检测证据；

b） 操作系统的安装应遵循最小化原则，及时进行升级和打补丁；

c） 域名解析软件的安全性应定期跟踪并及时升级和更新，防止漏洞带来的威胁；

d） 对业务、应用软件、服务器、网络设备等子系统进行7×24h不间断探测监控，监测的频率应不低于10min一次，监控日志的保存时间应至少为3个月。

e） 对域名资源记录和解析结果进行正确性抽检，抽检频率建议至少每小时1次。

7.6 通信和操作管理要求

7.6.1 操作程序和职责

a） 与公共域名解析系统相关的操作应有成文的操作程序，例如计算机启动和关机程序、备份、设备维护、介质处理、计算机机房、DNS软件的配置维护和物理安全等；

b） 与公共域名解析系统相关的各类责任及职责范围应加以分割，以降低未授权或无意识的修改或者不当使用域名解析系统资产的机会。

7.6.2 防范代码

防范恶意代码要基于恶意代码监测、修复软件、安全意识、适当的系统访问和变更管理控制措施，可以考虑以下内容：

a） 建立禁止使用未授权软件和正确使用授权软件的策略；

b） 安装和定期更新恶意代码检测和修复软件来扫描域名解析系统，并根据扫描结果升级域名解析系统。

c） 制定适当的从恶意代码攻击中恢复的业务连续性计划。

7.6.3 设备和线路备份

a） 系统应为分布式广域部署，节点间服务互备；

b） 关键设备的重要部件应采用冗余的方式提供保护；

c） 系统关键设备、重要线路应采用冗余的保护方式，提供灾难备份和恢复的能力；

7.6.4 数据备份

a） 应根据风险评估的结果，确定需要备份的数据和文件，一般情况下需考虑系统配置文件、解析日志、区文件等，备份时间至少为3个月；

b） 应建立备份拷贝的准确完整的记录和文件化的恢复程序；

c） 宜定期测试备份介质，以确保当需要应急使用时可以依靠这些备份介质；

d） 恢复程序应定期检查和测试，以确保他们有效，并能在操作程序恢复所分配的时间内完成；

7.6.5 网络安全管理

a） 应建立远程设备管理的职责和程序；

b） 主域名解析系统、辅域名解析系统以及备份解析系统的部署应处于不同自治域，避免单一网络失效引起的解析中断。

c） 宜建立专门的控制，以保护在公网上传递数据的保密性和完整性，并且保护已连接的系统及应用；

d） 如有必要，应按照相关标准要求，阻断或重定向用户对恶意域名的访问；

e） 应使用适当的日志记录和监视措施；

7.6.6 审计和分析

a） 应产生记录用户活动、异常和信息安全事态的审计日志，并要保存至少3个月以支持将来的调查和访问控制监视；

b） 应采取措施保证主域名解析系统、辅域名解析系统、备份域名解析系统内设备之间的时间同步，实现日志时间的精确同步；

c） 审计的内容至少包括：授权访问、特殊权限操作、未授权的访问尝试、系统警报或故障；

d） 记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。

7.7 访问控制管理要求

7.7.1 公共域名解析系统对外公开服务的访问控制

公共域名解析系统对外开放服务只开放UDP53端口。

7.7.2 访问控制策略和用户访问管理

a） 应在访问控制策略中清晰地规定每个用户或每组用户的访问控制规则和权利；

b） 应限制和控制特殊权限的分配及使用，防范未授权访问的多用户系统应通过正式的授权过程使特殊权限的分配受到控制；

c） 应定期检查权限的分配，确保用户访问权限的正确分配。

7.7.3 网络访问控制

a） 应能为数据流提供明确的允许/拒绝访问的能力，控制粒度为网段级；

b） 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；

c） 应在网络中实施路由控制，以确保计算机连接和信息流不违反业务应用的访问控制策略。

7.7.4 操作系统访问控制

a） 登录到操作系统的程序应设计成使未授权访问的机会减到最小；

b） 所有公共域名解析系统的管理员和第三方人员（包括技术支持人员、操作员、网络管理员、系统程序员和数据库管理员等）应有唯一的、专供其个人使用的标识符（用户ID），应选择一种适当的鉴别技术（口令、令牌或智能卡）证实用户所宣称的身份，静态口令应满足一定的复杂性要求并且定期更换；

c） 在一个设定的休止期后，超时登录应清空会话屏幕，也可以设置关闭应用和网络会话。

7.7.5 信息和敏感系统访问控制

a） 应对设备重要信息资源设置敏感标记；

b） 依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

c） 应实现操作系统和数据库系统特权用户的权限分离。

7.8 连续性管理要求

7.8.1 连续性管理的制定

a） 目标是防止公共域名解析系统的服务失效，保护公共域名解析系统免受重大失误或者灾难的影响，并且在遇到灾难的情况下及时恢复解析服务；

b） 应为公共域名解析系统制定一个解析服务连续性管理的过程，识别可能引起解析服务中断的事态以及这种事态发生的概率；

c） 应为公共域名解析系统制定一个解析服务连续性计划，来保持域名解析服务的可用性，在解析服务中断的情况下能够在要求的时间内恢复系统的服务。

7.8.2 制定连续性计划考虑的方面

a） 冗余方面：设备处理能力、关键设备及其重要部件、网络接入、系统的广域分布；

b） 数据及业务备份方面：关键数据和重要信息的备份和备份频率、业务状态的保护和恢复、业务系统的完整备份；

c） 应急处置预案方面：应制定应急处置预案，并定期对应急预案进行及时修订、修订期不低于1年；每年应进行不低于1次的应急预案演练。