SAC132

域名系统 (DNS) 依托自由与开放源码软件 (FOSS) 运行

ICANN 安全与稳定咨询委员会 (SSAC) 报告
2025 年 9 月 25 日

序言

这是 ICANN 安全与稳定咨询委员会 (Security and Stability Advisory Committee, SSAC) 向 ICANN 董事会、ICANN 组织、ICANN 社群以及更广泛的互联网社群提交的一份报告，旨在阐述域名系统 (Domain Name System, DNS) 对自由与开放源码软件 (Free and Open Source Software, FOSS) 的依赖机制。

SSAC 主要负责处理互联网名称和地址分配系统安全性与整合性的相关事务。具体包括：运营类事务（例如，与正确、可靠运营根区发布系统相关的事务）、技术管理类事务（例如，与地址分配、互联网号码分配相关的事务），以及注册类事务（例如，与注册管理机构和注册服务机构的服务相关的事务）。SSAC 持续针对互联网名称和地址分配服务展开威胁评估和风险分析，识别影响系统稳定性和安全性的主要威胁，并据此相应地向 ICANN 社群提出建议。SSAC 不具备监管、强制执行或裁定的职权。这些职能属于其他机构，本报告中提供的建议应根据其优缺点予以评估。SSAC 成员以个人身份参与委员会工作，不代表其所属雇主或其他任何组织。SSAC 就某份文件达成共识的条件为：文件所列作者就文件内容及建议达成一致，并且除文件末尾注明撤回的成员之外，其余 SSAC 成员最终均无异议。

目录

图示列表

表格列表

执行摘要

域名系统 (DNS) 是一个全球分布式、分层且去中心化的系统，其信息为几乎所有的在线交互提供支撑。其主要目的是将用户友好型域名映射到在网络上查找资源所需的计算机友好型 IP 地址。无论是浏览网页、发送电子邮件还是使用移动应用，所有在线连接都依赖于由 DNS 生成并结构化的信息。

本报告的核心结论为：DNS 依托自由与开放源码软件 (FOSS) 构建并维持运行，这并非个别案例，而是普遍现状。对于 DNS 基础设施的最基本组件，采用 FOSS 已是常态。例如，在运营互联网根服务器系统 (Root Server System, RSS) 的 12 家独立组织中，至少有 9 家完全采用 FOSS 技术实现；在 10 家最大的顶级域 (Top-Level Domain, TLD) 服务提供商中，同样有 9 家使用 FOSS。这种主导地位源于 FOSS 开发模式的固有优势，它兼具经济效率和低门槛落地性，同时具备关键基础设施所需的透明度、协作安全性和运营弹性。

尽管 FOSS 开发模式与专有软件的开发模式存在本质区别，但 FOSS 本身的安全性并不本质上高于或低于专有软件。任何软件项目的安全性都是由其开发和维护流程的质量决定的，而不依赖于源代码的可见性。与商业软件不同，FOSS 是一项全球协作成果，以四项基本自由为原则：自由使用、自由研究、自由分享和自由修改。这个生态系统依赖于一个由维护者和贡献者组成的全球网络，他们通常都是无偿志愿者。尽管大量参与者为无偿志愿者，但 DNS 领域的独特之处在于，它同时依赖于少数几家长期存在的专业维护组织。这形成了一种基于社群协作的模式，而非传统软件供应链所依赖的商业合同模式。这种模式也带来了独特的风险：一是维护组织面临的财务可持续性问题，二是志愿维护者面临的职业倦怠问题。

这些独特属性意味着，针对专有软件设计的监管框架可能并不适配 FOSS，进而可能会对关键互联网基础设施的稳定性造成严重的意外后果。为应对这些复杂挑战并构建安全的数字化生态系统，安全与稳定咨询委员会 (SSAC) 为政策制定者提供以下指导方针：

- **认可 FOSS 的关键作用：**政策制定者应在相关立法或法规中明确载明，关键互联网基础设施依赖 FOSS，而对 FOSS 的运用是一项值得维护与强化的优势。
- **咨询 FOSS 社群：**制定相关立法和法规时，应广泛征询 FOSS 生态系统的各方意见，涵盖个人维护者、非营利组织和企业。
- **借鉴 FOSS 监管领域的当代案例：**政策制定者可参考报告所收录、体现当代监管实践的最新案例研究，这些实践已融入了 FOSS 开发模式的独特属性。
- **激励 FOSS 可持续发展：**鼓励公共和私营部门为关键 FOSS 项目提供支持，以此助力共享公共利益的建设。
- **共同应对系统性风险：**促进和资助覆盖整个生态系统范围内的协作解决方案，缓和共享型依赖关系引发的风险，避免给个人维护者增加负担。

1 简介

本报告的撰写背景是，政策制定者正越来越多地参与行业行动，以减少数字基础设施中的软件漏洞。鉴于世界各国政府和监管机构均在着力保障软件供应链安全，开展这些工作的前提是，必须清晰理解互联网核心底层础系统的实际构建和维护机制。近期，旨在减少数字基础设施中软件漏洞的（拟议）监管举措包括：

- 英国软件供应商的自愿性软件安全实践准则。[1]
- 供美国政府使用的、关于安全软件开发实践的行业自我认证。[2]
- 欧盟对数字产品（包括软件）的市场准入要求（“网络弹性法案 (Cyber Resilience Act, CRA)”）。[3]
- 欧盟数字基础设施提供商的风险管理和报告义务（“NIS2 IA”）。[4]
- 开源社群被列为中国信息技术五年规划的发展目标之一。[5,6]

尽管自由与开放源码软件 (FOSS) 已是当今主流的软件开发实践，但其独特属性在政策讨论中却常被忽视。如果政策制定者在未充分理解 FOSS 独特的开发和供应模式的情况下引入监管举措，可能会威胁到依赖 FOSS 的关键基础设施的安全和稳定，包括互联网的域名和路由系统。本报告旨在提供必要的背景信息。

与其他行业的普遍情况不同，支撑互联网运行的大量软件均采用 FOSS 许可证授权。这些许可的核心不在于成本，而在于自由。具体来说，FOSS 许可证赋予基础设施运营商四项基本自由：自由使用、自由研究、自由修改，以及自由与他人分享软件（无论是否经过修

[1] “软件安全实践准则”。英国科学、创新和技术部，2025 年 5 月 7 日。https://www.gov.uk/government/publications/software-security-code-of-practice/software-security-code-of-practice。

[2] “安全软件开发认证表”。美国网络安全和基础设施安全局，https://www.cisa.gov/secure-software-attestation-form。

[3] “网络弹性法案：欧洲议会议员通过了旨在提升数字产品安全性的计划”，欧洲议会新闻稿，2024 年 3 月 12 日，https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products

[4] “网络弹性法案：欧洲议会议员通过了旨在提升数字产品安全性的计划”。新闻稿。欧洲议会，2024 年 3 月 12 日。https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products。

[5] “‘十四五’软件和信息技术服务业发展规划”。中华人民共和国国务院工业和信息化部，2021 年 12 月。https://www.gov.cn/zhengce/zhengceku/2021-12/01/5655205/files/a44b507d67c74591ad4f5e55b98c4518.pdf。

[6] “译本：14th Five-Year Plan for National Informatization（国家信息化‘十四五’发展规划）”。斯坦福大学 DigiChina 项目，2022 年 1 月 24 日。https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/。

改）。这是一种开发模式，而非单纯的“免费”软件，[7]它为全球协作共建与维护大量互联网关键基础设施的基础。

本报告旨在帮助政策制定者全面理解 FOSS 在域名系统 (DNS) 和域名注册生态系统中的作用。

- 第 2 节提供了一个非技术性的 DNS 入门指南，介绍了这一关键基础设施的主要组件和功能。
- 第 3 节详细介绍了 FOSS 模式，对比专有软件，剖析其关键特性、固有优势和独特风险。
- 第 4 节介绍了安全与稳定咨询委员会 (SSAC) 关于 FOSS 普及度的核心研究，展示了 FOSS 在 DNS 核心环节中的主导地位。
- 第 5 节考察了美国、英国和欧盟的几个当代案例，展现政策制定者如何调整网络安全法规，以适配 FOSS 生态系统的独特现状。
- 第 6 节将报告的核心分析汇总为一系列结论，为后续第 7 节的指导方针提供证据基础。
- 第 7 节为政策制定者提供了直接、可行的指导方针。

2 DNS 入门指南

当您发送电子邮件、浏览网页或与朋友聊天时，您的设备（如计算机、手机或平板电脑）会收发海量信息。这一过程可以类比为数字明信片：包含发送地址、接收地址和具体内容。每台接入互联网的设备，都拥有至少有一个唯一的互联网协议 (Internet Protocol, IP) 地址。对人类而言，记忆名字比记忆数字更轻松。DNS 就如同互联网的地址簿，它将 IP 地址与域名建立映射，让所有人都能更便捷地访问互联网。[8,9] DNS 是一项关键系统，对保障全球互联网的持续稳定、安全和互操作性至关重要。

DNS 提供从用户友好型域名（例如，icann.org）到计算机友好型数字 IP 地址（例如，192.0.43.7 或 2001:db8::1）的映射。这些映射共同构成了全球域名空间。若要使网站或电

[7] FOSS 可以用于任何用途，并且不受许可证到期或地域限制等约束。任何人都可以研究其代码，无需签署保密协议或受到类似限制。它能够以几乎零成本的方式分享和复制。此外，任何人都可以修改 FOSS，且修改后的成果可以公开分享。若上述四项自由中至少其中一项自由缺失或受限，则该应用程序属于专有软件，而非开源软件。软件许可证赋予了四项自由。软件许可证规定了程序的使用和重复条件。要成为自由软件，其许可证文本必须至少包含上述四项自由。自由软件基金会 (https://www.gnu.org/licenses/license-list.html)、开放源代码促进会 (https://opensource.org/licenses) 和 Debian 项目 (https://wiki.debian.org/DFSGLicenses) 维护着经过审核和批准的许可证清单。如果某个应用程序的许可证未列入上述清单，则通常不能将其视为 FOSS。

[8] ICANN。“域名系统”，2022 年 9 月 13 日。https://www.icann.org/resources/pages/dns-2022-09-13-en。

[9] Cloudflare。“什么是 DNS？| DNS 的工作原理”，https://www.cloudflare.com/learning/dns/what-is-dns/。

子邮件账户可通过域名访问，域名持有人必须发布该服务对应的映射关系。通过 DNS 中的这一发布机制，域名与对应服务的 IP 地址的映射关系将对所有互联网用户开放。

如图 1 所示，DNS 生态系统包含三个主要部分：

- 域名注册（浅蓝色框）：这是用于获取域名的管理与合约框架。
- DNS 基础设施（绿色框）：这些技术系统通过将域名解析为 IP 地址，确保域名可在互联网上正常运行。
- 最终用户和内容服务（橙色和深蓝色框）：这些都是人们最终会使用的服务，例如网站和电子邮件。

本报告聚焦于域名注册和 DNS 基础设施，二者共同构成了互联网关键基础设施的核心层级。全球域名空间中的信息查询大多不以盈利为目的，而是向用户“免费”开放。支撑这一全球分布式服务能够作为“非营利性公共产品”运行的基础设施，即本报告所述的“DNS 基础设施”。该系统在互联网中广泛部署，由多个组件构成，并由多家独立组织运营；各组织在该系统中承担着不同的特定职能。这些系统具备互操作性，因为其接口和通信的必要技术细节已通过互联网工程任务组 (IETF) 实现标准化。

这一关键基础设施与其所传输的内容相互独立。注册域名并不等于创建网站，在 DNS 中发布域名以供访问，也不等于发布网站内容。本报告聚焦于支撑地址簿正常运行的底层软件，而非地址簿中记录的信息。

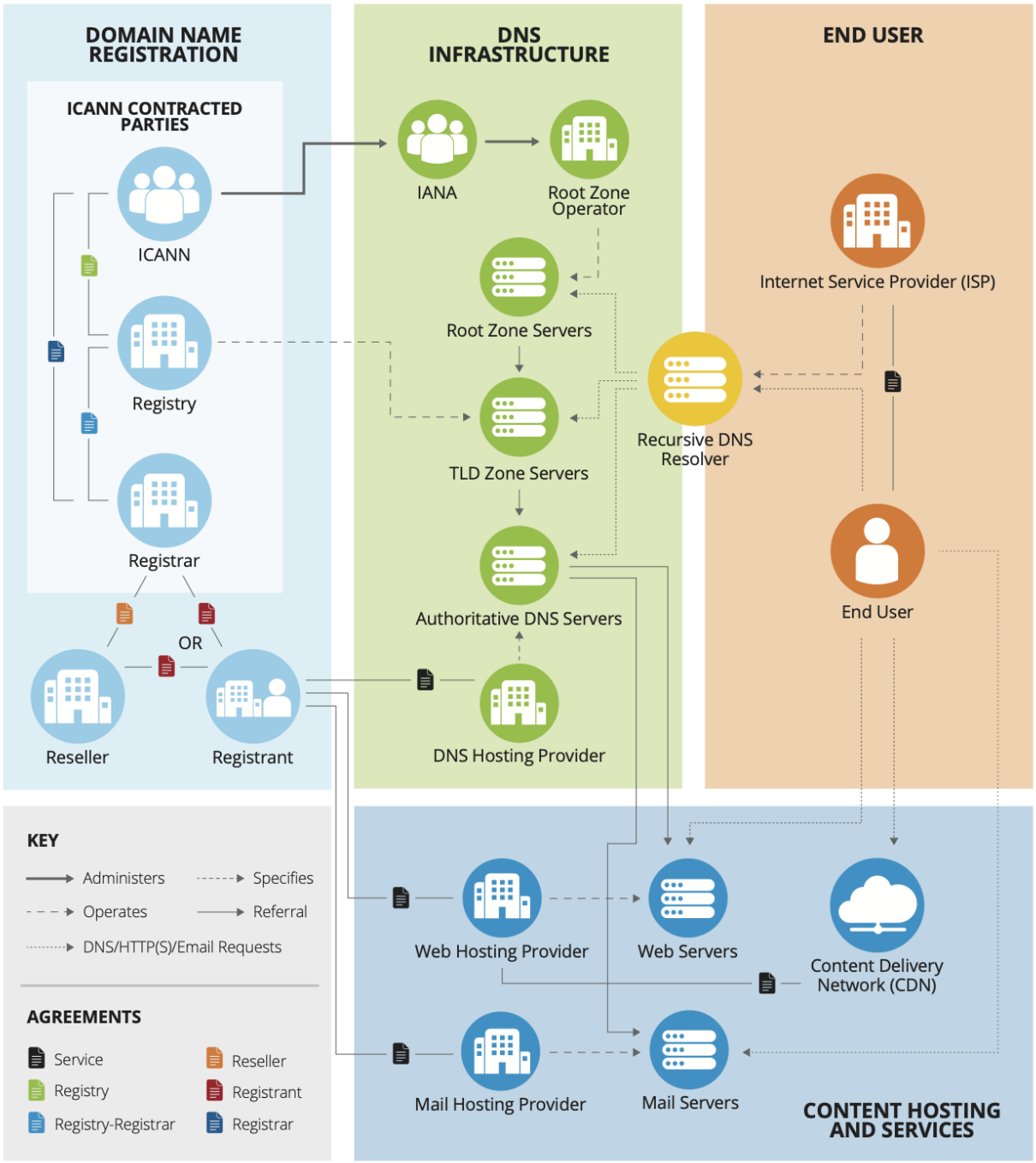

图 1： *互联网生态系统*。基思 • 德拉泽克 (Drazek, Keith)。“DNS 安全性：持续开展社群工作以缓和域名系统 (DNS) 安全威胁”。Verisign 博客，2021 年 12 月 7 日。https://blog.verisign.com/domain-names/ongoing-community-work-to-mitigate-domain-name-system-security-threats/。

2.1 DNS 层级结构

DNS 是一个全球分布式、分层且去中心化的系统。如图 1 中的“DNS 基础设施”所示，该系统旨在提高弹性，确保全球互联网不会出现单点故障。

图 2 展示了 DNS 域名空间的层级结构。

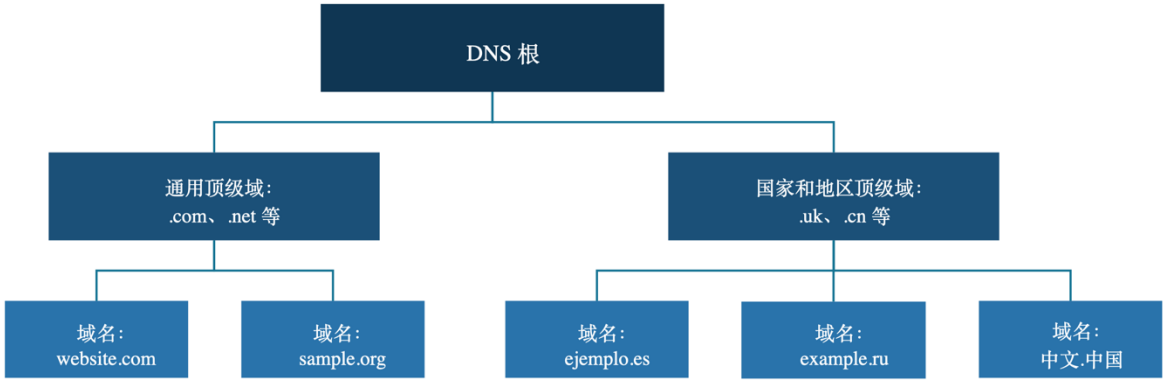

图 2：*DNS 层级结构*

层级结构的最顶端是 DNS 根域 (.)，由根服务器系统 (RSS) 提供服务。[10]根域指向各个顶级域 (TLD) 的权威服务器。TLD 是域名后缀，大致分为两类：

- 通用顶级域 (gTLD)：常见的通用顶级域包括 .com、.org、.xyz、 .shop 等。[11]
- 国家和地区顶级域 (ccTLD)：ccTLD 专为《ISO 3166-1 国家和地区代码清单》中列明的国家、地区和地理位置保留。[12] ccTLD 既可以基于 ISO 3166-1 标准所定义的双字母国家和地区代码来命名（例如：.jp 代表日本、.fr 代表法国、.ke 代表肯尼亚），也可以使用非 ASCII 字符的本地文字来代表国家或地区名称。[13]这类域名被称为国际化域名 (Internationalized Domain Name, IDN)，是 ICANN 自 2009 年起以来实施的一项概念。

在 TLD 之下是具体的域名，每个域名由两个或多个文本段构成，段与段之间以点号分隔。如图 3 所示，域名是从右到左构建的，首先是 TLD。例如，在 icann.org 中，TLD

[10] 根服务器系统由全球分布的服务器构成，由 12 家独立组织负责运营。如需了解根服务器运营商的更多信息，请参阅《RSSAC023v2：根服务器系统发展史》。ICANN 根服务器系统咨询委员会 (Root Server System Advisory Committee, RSSAC)，2020 年 6 月 17 日。https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf。
[11] ICANN。“缩略语和专有名词，通用顶级域 (Generic Top-Level Domain, gTLD)”，https://www.icann.org/en/icann-acronyms-and-terms/generic-top-level-domain-en。
[12] 国际标准化组织。“ISO 3166 — 国家和地区代码”，https://www.iso.org/iso-3166-country-codes.html。
[13] ICANN。“缩略语和专有名词，国家和地区顶级域 (Country Code Top-Level Domain, ccTLD)”，https://www.icann.org/en/icann-acronyms-and-terms/country-code-top-level-domain-en。

是 .org，二级域是 icann。它们共同构成唯一的域名。在第二个例子 bbc.co.uk 中，TLD 是 .uk，二级域是 .co。这种分层且去中心化的系统使全球互联网具有强大的稳定性和弹性。

域名是一种构成统一资源定位符 (Uniform Resource Locator, URL) 的唯一名称，使得人们能够在互联网上查找资源。域名自身代表着互联网上的一个特定地址，该地址属于一个实体，例如：企业、组织、机构或个人。[14]

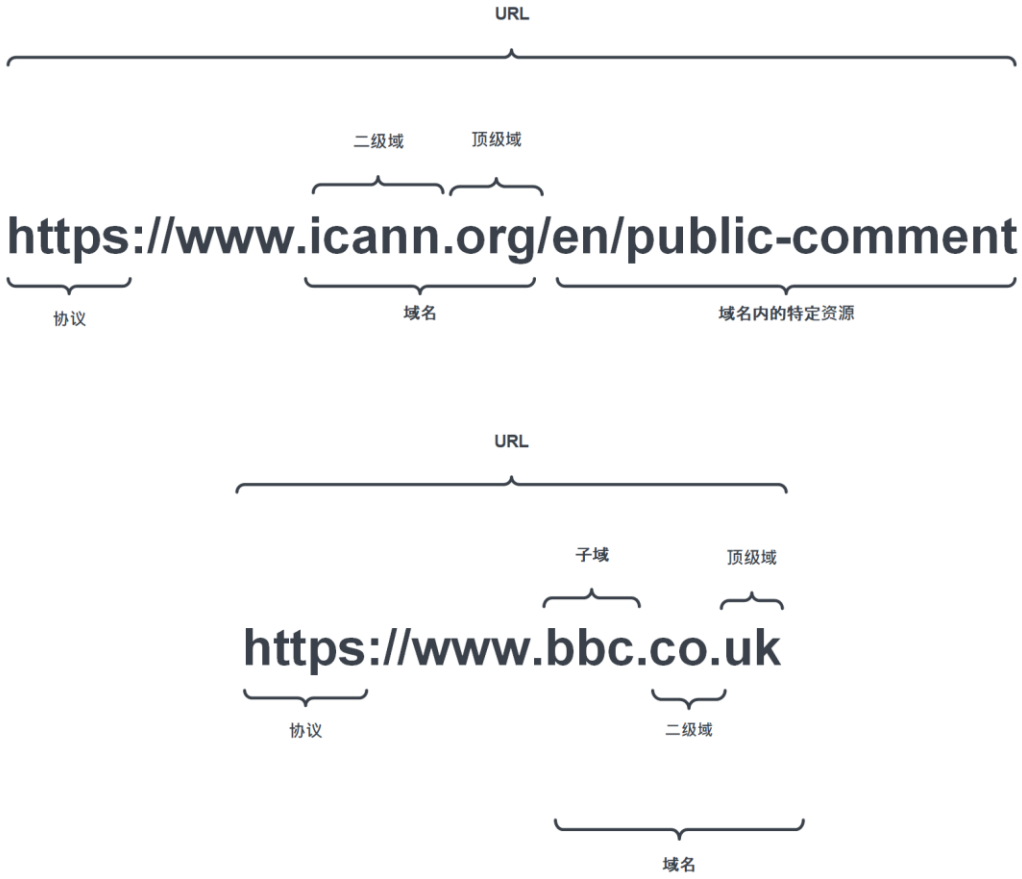

图 3： *URL 和域名的组成部分*

2.2 域名注册和发布

域名注册基础设施是指用于支持获取唯一域名的系统。如图 1 的“域名注册”部分所示，该流程涉及多个关键参与方和两个独立环节：注册和发布。

注册是指预留并获取域名的过程。注册人是指注册并拥有特定域名所有权的个人或组织。要在特定 TLD 下注册域名，注册人必须使用注册服务机构。注册服务机构是面向公众的机构，在域名体系中扮演零售商的角色。注册服务机构实际上是注册的分销渠道，负责处

[14] ICANN。“缩略语和专有名词，域名”，https://www.icann.org/en/icann-acronyms-and-terms/domain-name-en。

理付款、续订和其他管理信息。注册服务机构随后会与注册管理机构进行交互。注册管理机构是对应 TLD 中所有域名的权威性主数据库，维护此数据库的机构称为注册管理运行机构。为了自动完成他们之间的数百万笔交易，注册服务机构和注册管理机构采用了可扩展供应协议 (EPP)，这是一种用于域名注册、续订和转让的标准化协议。

注册成功后，域名的 DNS 记录将被发布至 DNS 基础设施中的权威服务器，从而使该域名可在互联网上访问。发布是指将域名的 DNS 记录部署到权威域名服务器上的技术过程。这些服务器保存着用户友好型域名与对应计算机友好型 IP 地址的映射列表，这对于定位以及验证网站、邮件服务器和其他互联网资源的真实性至关重要。

2.3 DNS 解析

当您在网页浏览器中输入 www.example.com 这类域名时，就会触发一个名为“DNS 解析”的流程。该流程依赖两类协同工作的 DNS 基础设施组件：递归解析器和权威服务器（参阅图 4）。

图 4：*传统 DNS 解析*

权威服务器是发布域名信息的组件，保存着特定域名的最终官方记录，并支持公开检索。权威域名服务器由个人、企业、大学、服务提供商和政府机构运营。例如，TLD 域名服务器会发布其注册管理机构内所有单个域名的技术数据。许多组织部署了本地 DNS 服务，这些服务仅提供其内部适用的信息，例如用于在企业内网中定位部门网站。这是 DNS 体系的重要组成部分，在公共互联网上不可见。

部分终端用户和小型企业依靠其域名注册服务机构或网络托管商的权威服务来发布其域名信息，但企业、政府和组织通常会独立运行其权威服务器，或自行部署，或外包托管。可靠性和冗余性是核心诉求；因此，负责管理发布于域名之下“区”(zone) 信息的管理员，通常会从外部提供商处采购“辅助权威 DNS 服务”。这些提供商会发布与主权威 DNS 服务器完全一致的数据。许多提供此类服务的机构，同时也为 TLD 提供权威 DNS 服务。

解析器用于辅助检索 DNS 信息，通过代表用户的设备（即“客户端”，如智能手机）发起查询，以获取正确的 IP 地址。为提升查询效率，解析器会维护一个持续更新的近期查询记录数据库，即缓存。在实际场景中，解析器通常会从本地缓存响应高达 90% 的查询，这一速度远快于通过互联网查询远端服务器。若缓存未命中所需内容，解析器则需要向权威服务器发起查询。解析器通常是负载极高的繁忙系统，部分原因在于持续的高流量可确保了缓存得到及时更新。

全球共有数以百万台解析器。解析器功能既可以部署在用户网络或接入提供商的本地网络中，也可以部署在云端，作为托管于互联网的独立服务，或与其他云服务协同运行。无论服务采用何种部署方式，都必须确保仅授权用户可以访问该服务。若该服务向互联网公众开放，则可能被滥用，例如遭受分布式拒绝服务 (Distributed Denial of Service, DDoS) 攻击。用户设备中的配置通常会决定其首选解析器提供商。许多高校、企业和互联网服务提供商 (ISP) 会为其内网用户提供本地解析器，此外还有 Google (8.8.8.8)、Quad9 (9.9.9.9)、Cloudflare (1.1.1.1) 等主流公共解析服务。选择解析器提供商的关键因素包括组织政策、解析器的过滤或拦截策略，以及加密 DNS 传输的可用性。解析流程（见图 4）展示了这些组件如何依据 DNS 层级结构协同运作。

3 FOSS 模式：关键特性和影响

上一节概述了 DNS 和域名注册基础设施，这些是支撑用户访问互联网的核心系统。本节将阐述这一关键基础设施的构建和维护方式。支撑该基础设施大部分组件的软件为自由与开放源码软件 (FOSS)，其开发模式与经济模型与传统专有软件存在本质区别。要开展严谨的政策讨论，必须理解这些独特的属性。

3.1 FOSS 生态系统中的关键角色

与传统闭源软件由单一主体内部开发不同，FOSS 模式采用开放且分布式的协作方式。这些角色并非互斥，任何人都可在任何场景下同时承担多个角色。在本报告中，将使用以下术语：

- **维护者：**负责 FOSS 项目整体方向的个人或团体。维护者有权决定是否接受社区对软件官方版本的贡献内容，从而确保软件的质量和一致性。他们是项目的管理者。
- **贡献者：**为项目提供改进的个人或组织，例如提交代码、文档或错误报告。所有贡献内容需经维护者审核通过后，才能被纳入官方项目版本。
- **用户或运营商：**指部署和使用软件的个人或组织。在 DNS 的语境下，“运营商”特指运行 DNS 基础设施组件（如权威服务器或解析器）的实体。用户和运营商是生态系统的重要组成部分，他们提供反馈并为项目赋予实际意义。

为了避免歧义，本报告使用“维护者”和“贡献者”这两个具体术语，而非泛指的“开发者”，因为同一主体可能同时以维护者、贡献者或独立开发者的身份参与代码编写。

3.2 FOSS 开发模式的核心原则

FOSS 模式的核心原则由其开源许可证所赋予的各项权利来定义。一个软件若要被视为 FOSS，其许可证必须向用户赋予四项基本自由：[15,16]

- 自由***使用***：可出于任何目的使用软件，不受许可证过期、地域限制等约束。
- 自由***研究***：可研究程序的工作原理，这需要在无需签署保密协议的情况下获取源代码。
- 自由***分享***软件，这意味着几乎可以无任何成本地重新分发和复制软件。
- 自由***修改***：可自由修改程序并向公众发布这些改进成果。

若上述任何一项自由缺失或被削弱，该软件即被视为专有软件，而非 FOSS。这些自由构成了 FOSS 一般特性的基础，与专有软件形成显著差异。自由软件基金会[17]、开放源代码促进会[18]和 Debian 项目[19]等组织维护着经审核并批准的软件许可证清单，确保其符合上述标准。

这四项自由并非抽象的原则；而是 FOSS 独特开发模式和经济特征的基石，其具体体现将在以下小节中阐述。

3.2.1 FOSS 模式支持全球合作开发

由于 FOSS 许可证允许任何人研究、修改和分享代码，因而促成了软件开发领域的开放式全球协作。在 FOSS 开发中，不会对贡献者施加任何预设的准入条件，任何个人都可以为软件贡献内容。贡献者背景多元，既可以是企业产品开发的一部分，也可以是个人的自发行为。

最终产生的产品可供任何人自由获取，可用于任何用途（包括商业用途），并支持进一步的开发迭代。这降低了软件演进过程中的阻力，特别是当修改被整合回软件产品时，能够加快功能开发并更快地修复软件缺陷和安全问题。FOSS 的协作性质促进了透明度和快速创新。此外，贡献内容本身通常也是开放的，允许其他人检查提议的贡献内容，并就贡献内容的适用性以及将贡献内容整合到软件产品所带来的优势发表意见。

[15] GNU 操作系统。“什么是自由软件？”，https://www.gnu.org/philosophy/free-sw.html。
[16] 另一个广受认可的 FOSS 许可定义是开放源代码促进会提出的“开放源代码定义”，https://opensource.org/osd。
[17] GNU 操作系统。“各类许可证及其评论”，https://www.gnu.org/licenses/license-list.html。
[18] 开放源代码促进会。“OSI 批准的许可证”，https://opensource.org/licenses。
[19] Debian Wiki。“DFSGLicenses”，https://wiki.debian.org/DFSGLicenses。

不过，未经一定程度的检查和审核就全盘接受所有贡献内容的情况并不常见。此类检查的目的是降低因引入不一致、错误或恶意代码而导致软件受损的风险。接受贡献内容通常遵循一些通用规则，其中包括对版权和知识产权的保留要求。FOSS 的一项常见实践是，所有协作贡献内容不得在现有软件许可条款之外都不能在软件已有的相关条件之外，对软件的使用施加额外的限制，也不能对现有软件基础施加额外的版权或知识产权约束。

除了向原项目贡献内容，FOSS 许可证还允许贡献者创建自己的衍生版本（即分支），而非继续参与上游项目。无约束分支可实现快速创新。部分分支的受欢迎程度甚至超过了其上游版本。但分支也可能导致混乱，分散有限的审核资源，从而影响对错误或恶意代码的发现。

软件既可以是独立封装的，也可以依赖其他软件库来实现必要的功能。这些库本质上是外部代码组件，其变化可能不会被主项目开发者及时察觉，从而导致意外行为。由于 FOSS 作为组件被集成到其他软件（包括专有软件）的门槛很低，尽管此类风险并非 FOSS 独有，但在 FOSS 场景中发生的频率更高。

3.2.2 FOSS 模式在没有合同关系的情况下运作

FOSS 供应模式的一个核心特点是，各方之间通常不存在任何合同关系。这与实体商品的供应链形成鲜明对比，在实体商品供应链中，制造商和分销商通过合同来附加政策或转移合规义务。然而，在 FOSS 供应模式下，运营商可以通过多种途径获得软件。虽然维护者会以源代码形式提供软件供公众下载，但更常见的情况是，软件通过中间渠道分发，例如提供可安装软件包的“Debian 项目”，或是其他产品或服务的中间商。除了维护者的开源许可条款之外，运营商很少会与此类中间商签订任何合同，只会与维护者签订少数合同。若存在合同关系，通常也是为了获取技术支持，而非针对 FOSS 软件本身。

3.2.3 FOSS 模式使资金与使用脱钩

复制额外副本不会产生任何固有的材料成本。自由使用和分享 FOSS，意味着许可证无需金钱交易即可授予权利。用户，包括互联网基础设施的运营商，可以自愿资助 FOSS 的开发和维护，但许可证并不强制要求，因此开发者的资金来源与其软件的使用并不挂钩。

3.2.4 FOSS 通常没有单一责任法律实体

在实体商品领域，人们通常会假定存在单一责任法律实体，该实体又可能会受到政策约束，或承担合规义务。与实体商品不同，软件的全球分发通常可以通过互联网以极低或零成本进行。这使得个人或群体无需付费，也无需成立法律实体，即可编写和分发软件。Debian 项目[20]就是一个无关联法律实体的知名开源项目示例。Debian 软件应用于核能、铁路运输、工业自动化和医疗设备等领域。虽然部分 FOSS 项目设有法律实体来提供治理、

[20] Debian。“我们的理念：我们为什么要做，我们如何去做”，https://www.debian.org/intro/philosophy。

赞助甚至雇佣支持，但大多数项目都没有。我们稍后会看到，DNS 在这方面比较特殊，有四家小型组织专业维护 FOSS。

3.3 专有系统依赖于 FOSS

事实证明，FOSS 的特性与那些本身是专有（非 FOSS）的系统也息息相关。这是因为现代专有系统通常依赖于 FOSS 才能运行。FOSS 工具和库在专有软件的开发和部署中无处不在。例如，大多数软件的生成都离不开编译器或运行时环境；软件无法在没有对象存储或数据库的情况下存储对象或结构化数据；软件无法在没有消息传递机制的情况下与其他组件进行通信。这些后端功能通常由 FOSS 提供。

就 DNS 而言，Cloudflare 提供了一个很有用的例子。Cloudflare 运营着一项广泛使用的公共 DNS 解析器服务，该服务称为“1.1.1.1”。该服务最初基于 FOSS 软件 Knot Resolver 成功运营；然而后来被内部开发的专有软件所取代。[21]1.1.1.1 核心运行的专有软件是用 Rust 编写的，Rust 是一种编程语言，其规范、参考实现和编译器由非营利基金会作为 FOSS 提供。[22]它还使用 tokio，[23]一个同样是 FOSS 的异步运行时。它在 FOSS 操作系统 Linux 上运行，同时还依赖大量其他 FOSS 组件，这些组件提供可观测性和其他运营必备功能。[24]Cloudflare 1.1.1.1 背后的专有软件得以大规模运行，正是得益于 FOSS，而非与之无关。

3.4 FOSS 在 DNS 生态系统中的固有优势

FOSS 模式不仅仅是一个理论构想；其原则将转化为切实的好处，使其成为 DNS 基础设施软件的主导范式。研究、分享和改进软件的自由共同营造出一个可促进透明度、弹性和创新的环境。这些并非偶然的副产品，而是 FOSS 模式固有的优势，已被证明特别适用于满足构建和维护关键互联网基础设施的需求。以下各节将详细介绍这些具体优势。

3.4.1 透明度和合作安全性

开源 DNS 实现受益于透明度。FOSS 实现的源代码的可用性使得全球开发者、研究人员和运营商社群能够识别并解决漏洞，而且通常比在专有系统中更快地解决漏洞。几十年

[21] 安邦 • 温 (Wen, Anbang) 和马雷克 • 瓦夫鲁沙 (Marek Vavruša)。“Rust 和 Wasm 如何驱动 Cloudflare 的 1.1.1.1”。Cloudflare 博客，2023 年 2 月 28 日。https://blog.cloudflare.com/big-pineapple-intro/。
[22] Rust 基金会。“关于我们 - 使命、领导层、董事会”，https://rustfoundation.org/about/。
[23] Tokio。“教程”，https://tokio.rs/tokio/tutorial。
[24] 约翰 • 格雷厄姆-卡明 (Graham-Cumming, John)。“CloudFlare 和开源软件：一条双向道路”。Cloudflare 博客，2013 年 10 月 7 日。https://blog.cloudflare.com/open source-two-way-street/。

来，它们一直是学术和安全社群积极研究的课题，[25]因而产生了大量 DNS 协议和开源实现方面的漏洞报告。[26]

如果发现漏洞，这三个群体之间的紧密联系可以确保及时解决任何严重问题，并协调漏洞披露和补丁发布，从而保证关键 DNS 服务器（例如根服务器）在信息公开之前得到全面保护，且所有其他服务器都能及时更新。

在对 DNS 基础设施运营商进行的一项调查中（参阅附录 C），受访者表示，他们重视供应链透明度所带来的可见性，认为这一强大特性使其能够快速修补所运营 DNS 服务依赖的软件中的漏洞。例如，请参阅以下回复：[27]

> 开源软件能够快速暴露任何缺陷，无论是安全相关缺陷还是其他方面的缺陷，并且补丁的发布和分发速度远快于任何商业实体。
>
> 诸如 [经过节选修订]、[经过节选修订] 和 [经过节选修订] 等大型商业实体多年来经常在漏洞被发现很久之后才发布安全补丁。
>
> 我们始终主张使用 FOSS 符合所有人的利益，包括我们服务的用户和消费者。这样他们便能验证我们使用的软件组件是否可靠。在我们使用的软件中，如果极少数情况下检测到安全问题，我们会公开讨论并以最快的速度修复，这与我们看到的专有软件的情况截然不同。
>
> 专有软件存在安全问题的例子比比皆是，它们在透明度或问题修复方面的记录也往往不佳。在这两方面，FOSS 社群比大多数供应商表现都要好。

运营商在公共场合积极、公开地讨论 FOSS DNS 软件的使用和管理问题。每个主流的 DNS 软件系统都有一个开放的公共用户电子邮件清单，[28]以及一个全球都能访问的公共错误或问题数据库。[29]DNS 社群通过域名系统运营、分析和研究中心 (DNS Operations, Analysis, and Research Center, DNS-OARC)[30] 这一行业组织在运营和研究方面开展合作。

---

[25] 例如，请参阅保罗·维克西 (Paul Vixie) 的论文“DNS 和 BIND 安全问题”，该论文发表于*第五届 USENIX UNIX 安全研讨会论文集*，犹他州盐湖城，1995 年。https://www.usenix.org/legacy/publications/library/proceedings/security95/full_papers/vixie.pdf。

[26] 为了说明“积极研究的课题”这一概念，请参阅陆超逸 (Chaoyi Lu) 所作的关于 2024 年发表的 23 篇 DNS 安全研究论文的研究结果总结，“2024 年发表的 DNS 和安全学术论文综述”（演示文稿，ICANN82，华盛顿州西雅图，2025 年 3 月 12 日），https://static.sched.com/hosted_files/icann82/7b/1.1%20chaoyi-dnspapers2024-0304.pdf。

[27] ICANN 安全与稳定咨询委员会，“ICANN SSAC 关于开源监管对 DNS 基础设施预期影响的调查”，个人通信，2025 年 2 月。

[28] 例如，请参阅 CZnic (https://lists.nic.cz/postorius/lists/knot-resolver-users.lists.nic.cz/)、NLnet Labs (https://www.nlnetlabs.nl/support/mailing-lists/) 和 PowerDNS (https://mailman.powerdns.com/mailman/listinfo/) 的公共电子邮件清单。

[29] 例如，请参阅 CoreDNS (https://github.com/coredns/coredns/issues) 和 BIND 9 (https://gitlab.isc.org/isc-projects/bind9/-/issues/) 的问题跟踪。

[30] 域名系统运营、分析和研究中心。“DNS-OARC 简介”，2008 年 7 月 3 日。https://www.dns-oarc.net/oarc/info。

这种开放的沟通文化有助于更快、更广泛地了解运营问题、软件错误、各项实现之间的不兼容问题，以及影响系统其他部分的运营失误。

3.4.2 稳定性与长期支持

FOSS 通常普遍依赖志愿者维护，而且往往是由一个人维护。就 DNS 而言，四个领先的开源解决方案是由来自北美和欧洲多个国家和地区的四家不同组织（三家非营利机构和一家商业公司）开发的。[31]这四家组织都是在互联网普及之初成立的，并已实现收入来源和内部组织的稳定。这些组织各自通过编写新代码以及审查和审核来自全球各地活跃社群的贡献代码来主导其软件的开发。这些赞助组织的长期承诺以及对软件变更的集中技术控制，有助于缓和在缺乏强大技术控制的情况下开发的 FOSS 项目常见的质量、安全性和可靠性问题。开源 DNS 技术社群的文化决定了，渗透者需要付出长期且持续的努力，才能建立起担任可信角色所需的人脉与声誉。

3.4.3 通过多样化提升运营弹性

DNS 服务所需的高可用性意味着需要进行冗余配置并避免单点故障。对于许多运营商而言，这包括需要在软件中运行多个独立的 DNS 实现。选择外包服务的运营商也可以采取多供应商策略。这自然催生了对多种解决方案的内在需求，从而让高可靠性服务的运营商可以并行运行两套或更多方案，既避免依赖于单一软件开发者，也避免完全暴露在单一产品的问题风险中。FOSS DNS 软件的可用性降低了组织运营自身基础设施的门槛，为防止市场集中和中心化提供了一条出路。[32]

3.4.4 经济增长和创新的助推器

众所周知，FOSS 是增长的助推器。[33,34]正如我们所见，多种开源产品可供世界各地任何需要 DNS 软件的人免费使用。潜在用户包括 ISP、域名注册管理机构和注册服务机构以及互联网用户。可能无法负担专有软件许可费用的个人、非营利组织、初创企业和主题专

[31] 按字母顺序排序：CZNIC，捷克互联网服务提供商（“ISP”）协会，成立于 1998 年；Internet Systems Consortium, Inc.（“ISC”），美国非营利企业，成立于 1994 年，明确以支持互联网基础设施的开源软件和系统为宗旨；NLnet Labs，荷兰非营利组织，成立于 1999 年，致力于开发 DNS 和域间路由的开放标准和开源软件；以及 PowerDNS，荷兰公司，成立于 1999 年，支持为 ISP 开发专用 DNS 软件。

[32] 马克 • 诺丁汉 (Nottingham, Mark)。“RFC 9518：中心化、去中心化与互联网标准”。意见征询。互联网工程任务组，2023 年 12 月 18 日。https://datatracker.ietf.org/doc/rfc9518/。

[33] “分析估计成本效益率高于 1:4，并预测 OSS 贡献增加 10% 每年将额外带来 0.4% 至 0.6% 的 GDP 增长，并在欧盟催生 600 多家新的 ICT 初创企业。案例研究表明，公共部门通过采购 OSS 而非专有软件，可以降低总体拥有成本，摆脱供应商束缚，从而增强数字化自主性。”摘录自欧盟委员会通信网络、内容和技术总司发布的“*开源软硬件对欧盟经济的技术独立性、竞争力和创新的影响：最终研究报告*”。卢森堡：出版办公室，2021 年。https://data.europa.eu/doi/10.2759/430161。

[34] 莱特 (Wright)、娜塔莉娅 • 兰格伯德 (Nataliya Langburd)、弗兰克 • 纳格尔 (Frank Nagle) 和谢恩 • 格林斯坦 (Shane Greenstein)。“开源软件与全球创业”。《*研究政策*》第 52 卷，第 9 期（2023 年）：104846。https://doi.org/10.1016/j.respol.2023.104846。

家可以免费获得他们所需的软件。正如一位参与 DNS 运营商调查的受访者所说（参阅附录 C）：“我目前最大的担忧是，我们在技术栈的非关键部分使用了太多没有支持合同的开源组件，以至于即使存在可用的许可，我们也无法承担全部的许可费用。”[35]

多种 FOSS DNS 解决方案的存在对互联网使用以及在线软件和服务（包括开源和专有）的技术与商业发展具有积极影响。许多专有系统和托管服务严重依赖开源组件来实现关键功能；许多云计算和在线服务的专有平台都依赖某个 FOSS DNS 产品作为组件。[36]与此同时，大量 DNS 基础设施依赖 OpenSSL 等 FOSS 加密库。同样，开源操作系统 Linux 构成了相当一部分云基础设施、服务器环境和物联网 (Internet of Things, IoT) 设备的基础。这一基础性作用凸显了 FOSS 对技术创新的深远影响。专有软件常常会整合这些 FOSS 框架，并以此为基础构建闭源应用程序或功能，这样便在两种模式之间建立起共生关系。[37]

3.4.5 对数字化自主性的贡献

由于使用 FOSS 一般不需要支付许可费用或补偿金，因此，与使用专有软件相比，创办新的数字企业所需的资金可能更少。此外，FOSS 准许自由研究、修改和重新分发代码，这使本地知识和技能得以增长，从而产生新的研究和商业项目。本地定制或进一步开发不需要原作者的任何授权或同意。基于 FOSS 的任何服务都不会受到外国版权所有者的封锁，因为 FOSS 许可证不能撤销；即使在发生贸易冲突和禁运的情况下，代码仍然可以使用。

3.5 FOSS 模式的固有风险

尽管 FOSS 模式具有显著的优势，但其独有的特性也带来了一系列不同于传统专有软件的风险。这些并不是模式本身的缺陷，而是必须理解和应对的内在权衡，特别是当软件用于关键基础设施时。经济模式、开发的分布式性质以及缺乏传统的合同关系都会对长期可持续性和运营安全性产生影响。以下几节将详细介绍这些固有风险。

[35] ICANN 安全与稳定咨询委员会，“ICANN SSAC 关于开源监管对 DNS 基础设施预期影响的调查”。
[36] 目前，尚无独立的单一引证可支持此论断。然而，基于本文作者集体所做的调查，我们可以自信地说事实确实如此。公开披露具体哪个平台使用何种服务涉及保密性问题，因此，这是一个虽缺乏相应文档支持、但依据充分的陈述。
[37] 杰夫 • 戈特梅克 (Gortmaker, Jeff)。“产业均衡中的开源软件政策”。工作论文，技术报告，2024 年。https://jeffgortmaker.com/files/Open_Source_Software_Policy_in_Industry_Equilibrium.pdf。

3.5.1 财务可持续性和维护者职业倦怠

DNS 面临的主要威胁之一是 FOSS 普遍存在的财务可持续性问题。这种模式使资金与使用脱钩（第 3.2.3 节），这促成了广泛采用，但也导致了“搭便车”现象，[38]即整个世界可能都依赖于由少数人资助的软件。[39,40]

正如宽带互联网技术咨询小组 (BITAG) 的一份报告所指出的：

> 愿意购买带有昂贵支持合同的网络设备，却不愿资助开源软件，两者之间存在脱节，而在许多情况下，这些设备正是依赖于开源软件。通常情况下，网络运营商的技术人员愿意支持开发，但他们的企业结构却不允许他们这样做，因为这种软件不是人们可以购买的附带支持合同的封装产品。资助某项功能的开发也可能成为问题，因为法律部门的默认假设是软件开发会导致赞助商[独家]拥有知识产权，这与自由与开放源码软件模式相背离。[41]

虽然维护这四种领先的开源 DNS 实现的组织在财务和组织方面都实现了持续稳定，但他们都是小型组织。如果其中一家组织的资金来源受到威胁，或者如果法规施加的负担超出了其成本承受能力，那么组织就可能陷入不稳定。如果其中一个领先的开源系统维护不足或完全不可用，对 DNS 的影响可能是巨大的。

对于那些需要持续维护但又与其用户的主要业务流程脱节的基础工具来说，情况尤其如此。四种最主流的开源 DNS 实现由不超过十几名工程师组成的开发团队提供支持，因此，增加可能相当于一名全职员工工作量的项目要求将是一个巨大的负担。

付费维护者的资金来源多种多样，其中有些可能出乎意料。除了接受捐赠和提供私人技术支持外，一些项目还为资金支持者提供早期错误修复、对生命周期终止分支的支持、优先

[38] 贾斯汀-帕帕斯 • 约翰逊 (Johnson, Justin Pappas)。“微观经济理论文集”。麻省理工学院学位论文，1999 年。http://hdl.handle.net/1721.1/9518。

[39] 约翰 • 克里斯托夫 (Kristoff, John)，亚历山大 • 班德 (Alexander Band)、翁德雷 • 菲利普 (Ondrej Filip) 和杰夫 • 奥斯本 (Jeff Osborn)。*专家小组：核心系统 OSS 专家小组*。北美网络运营商集团第 84 次会议，2022 年。https://www.youtube.com/watch?v=vWiW-3jMw7w。

[40] 例如，一份报告强调了基本路由软件的使用与其开发资金贡献之间的失衡：“我们用两个例子来说明这种资助与使用之间失衡的相关性。在估计 2,000 个 Routinator RP 软件安装实例和 1,400 个使用 Krill 委托 CA 软件的网络中，为这两款软件的开发提供资助的机构不足十家。大多数运营商确实依赖这些软件的稳定性、持续存在和未来发展，但并没有为此做出贡献。”宽带互联网技术咨询小组 (Broadband Internet Technical Advisory Group, BITAG) 技术工作组，“互联网路由基础设施的安全性”，2022 年 11 月 2 日，第 26 页，https://www.bitag.org/documents/BITAG_Routing_Security.pdf。

[41] BITAG 技术工作组，“互联网路由基础设施的安全性”，第 26 页。

功能开发、访问预编译包和额外安全服务。[42,43,44,45]监管机构应注意，堵塞开源软件维护者为其运营筹集资金的任何可行渠道。

DNS 的 FOSS 非常特殊，因为确实存在长期雇佣维护者的组织。对于这些组织的持续存在，风险在于*财务*可持续性。但就普遍情况而言，风险在于动机。绝大多数 FOSS 由单个个人在业余时间维护。[46]DNS 软件的例子包括 Dnsmasq，这是一款最常嵌入家用和小型企业所用的廉价小型路由器中的 DNS 软件。它主要由一名基本无报酬的志愿者维护。[47]同样，几个成熟的 DNS 编程软件库实际上也是由单个个人在业余时间维护。[48]另一个主流 DNS 实现 CoreDNS 及其底层 Go DNS 库分别由社群和一名（专家级）志愿维护者提供支持。这些例子突显了软件生态系统的一个决定性特征：一个小型组织或单一开发者可以在全球数字基础设施所需软件的编写中发挥关键作用，同时他们的工作完全与运营该基础设施的资本或运营支出脱钩。对于这些独立的志愿维护者而言，除非这项工作成为他们主要的全职工作并获得资金支持，否则他们面临的风险不是财务可持续性问题，而是职业倦怠问题。监管机构应注意，不要施加超出维护者能力和意愿的额外负担，因为这些维护工作本质上只是他们业余爱好的项目。这一直是一个活跃的研究领域，政策制定者应充分关注学者们提出的建议。[49]

[42] 例如，互联网系统联盟提供早期漏洞通知服务。请参阅互联网系统联盟的“早期漏洞通知 (Early Vulnerability Notification, EVN)”，https://www.isc.org/evn/。

[43] NLnet Labs 通过其子公司 Open NetLabs 提供培训、咨询、技术支持和软件开发服务。请参阅 NLnet Labs 的“Open Netlabs 服务 - 咨询”，https://nlnetlabs.nl/services/consultancy/。

[44] PowerDNS 提供各种服务和产品，包括 PowerDNS Protect，这是一种包含保护性拦截清单的安全服务。请参阅“PowerDNS Protect”，https://www.powerdns.com/powerdns-protect。

[45] 有关各种开源组织模式的概述，请参阅“开源原型：有目的的开源框架”，Open Tech Strategies，Mozilla Corporation，2019 年 10 月 28 日，https://blog.mozilla.org/wp-content/uploads/2018/05/MZOTS_OS_Archetypes_report_ext_scr.pdf。

[46] 乔希 • 布雷瑟斯 (Bressers, Josh)。“开源软件由一个人维护”。Open Source Security，2025 年 8 月 28 日。https://opensourcesecurity.io/2025/08-oss-one-person/。

[47] “Dnsmasq - 小型网络的网络服务”，https://thekelleys.org.uk/dnsmasq/doc.html。

[48] 示例包括用于 Perl 编程语言的 *Net::DNS*，以及 *miekg/dns*，这是一个用于 Kubernetes、Docker 和 Let's Encrypt 认证机构的 Go DNS 库。更多库示例可在表 7 中找到。

[49] 纳迪娅 • 埃格巴尔 (Eghbal, Nadia)。“道路与桥梁：我们的数字基础设施背后不为人知的劳动”。福特基金会，2016 年 7 月 14 日。https://www.fordfoundation.org/work/learning/research-reports/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure/。

3.5.2 共享型依赖关系带来的供应链风险

包括 FOSS 和商业软件在内的大量关键软件都依赖于某些相同的 FOSS 组件。一个主流 FOSS 加密库中的严重错误[50]可能会影响所有 DNS 实现。[51]此外，还有其他一些不那么显眼的经常重复使用的组件。这不仅是 DNS、FOSS，也是整个软件领域中一个重大的潜在弱点。[52]上文第 3.5.1 节讨论的可持续性风险也适用于这些共享组件，从而加剧了威胁。

心怀恶意企图的 FOSS 贡献者可能会将恶意代码植入开源项目或其组件中而不被发现，这进一步加剧了风险。这些恶意代码可以通过篡改软件包存储库或作为项目的贡献内容引入。为了防止将恶意代码引入软件项目，在审查和监控代码依赖关系时必须保持警惕。

3.5.3 免费 FOSS 不提供任何保证，也不保证提供支持

免费提供的软件是一个很有吸引力的选择，因为它无需付费，通常只需下载软件包即可使用。但由于它不提供任何保证，也不承诺提供支持，因此使用时也存在风险。默认情况下，除了开源许可协议之外，FOSS 产品提供商和用户之间没有任何其他合同。[53]除非用户与维护者或其他方自行安排维护事宜，否则无法保证他们会获得主动维护或支持。

如果产品存在安全缺陷，无论是意外引入（如 OpenSSL 的心脏滴血[54]漏洞），还是恶意引入（如 xz Utils 后门[55]），都没有人有义务提供修复程序。虽然从技术上讲，包括用户在内的任何人都可以复制源代码并手动修正问题，但这种“分叉”需要大量的软件工程专业知识和运营资源，因此在大多数情况下，用户实际上无法控制修复程序的可用性。这个问题在 OpenSSL 和 xz 等软件包中尤为严重，因为这些软件包被广泛使用，没有容易获得的替代品。单一化风险并非开源领域独有，但这或许正是此类普遍风险同样适用于 FOSS 的原因之一。

社群对维护 FOSS 的兴趣下降，可能会促使一些组织通过签订合同提供维护服务。然而，这些支持组织对代码库的修改通常会提交到 FOSS 项目的上游，以尽量减少维护独立代码

---

[50] OpenSSL 就是一个被广泛依赖的加密库的典型例子。为了说明这种依赖关系的规模，以 OpenSSL 的“心脏滴血”漏洞为例，估计有 17% 经可信机构认证的互联网网络服务器被认为容易受到攻击。Netcraft，“50 万个广受信任的网站易受心脏滴血漏洞攻击”，*Netcraft 新闻*，2014 年 4 月 8 日，https://web.archive.org/web/20141119102520/http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html。

[51] 与 DNS 软件一样，开发加密软件也是一项专业工作。尽管存在一些长期使用的 FOSS 加密软件，但多样性和质量仍然是一个问题。

[52] 有关揭示共享型依赖关系的一次尝试示例，请参阅“第三次自由与开放源码软件普查”，*Linux 基金会*，2024 年 12 月：https://www.linuxfoundation.org/research/census-iii

[53] 认为维护者与运营商之间存在合同关系是一种普遍的误解，这一点已在第 3.2.2 节中予以阐明。

[54] “心脏滴血漏洞”，https://heartbleed.com/。

[55] 丹 • 古丁 (Goodin, Dan)。《险些波及全球的 xz Utils 后门事件：我们已知的信息》。Ars Technica，2024 年 4 月 1 日。https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost-infected-the-world/。

库的负担。反过来，这又使其他人在无需付费的情况下就可以从此类维护中获益。这就导致了一个“搭便车”的问题：当一家服务提供商使用 FOSS 却不为其维护做出贡献时，其成本可能低于那些参与贡献的竞争对手，从而以更低的价格抢占市场。[56]

缺乏固有保证或支持的问题可以得到缓和。运营商可以培训和保留员工的专业技能，资助或雇佣维护者，[57]或者签订支持合同以获得维护者或专家贡献者的专业技能。[58]第 3.5.1 节引用的 BITAG 报告举例说明了阻碍运营商这样做的组织障碍。

3.5.4 部署中的运营风险

FOSS 的分布式特性带来了与软件真实性验证、补丁管理和技能娴熟的运维人员短缺有关的运营挑战。

检查软件的真实性

FOSS 在互联网上自由分发，因此可能遭到劫持或被伪造代码取代。考虑到这种风险，FOSS 的维护者通常会使用强大的加密方法对软件进行签名。用户可以验证这些签名，以确保软件的完整性。互联网基础设施中使用的所有最主流的 FOSS DNS 实现都进行了签名。然而，用户可能不会检查这些签名，或者可能会通过不验证或以其他方式维护软件完整性的中介机构获取软件。

缺乏有关部署和修补速度的信息

研究人员对寻找 FOSS DNS 软件中的漏洞有着浓厚的兴趣，并且一直以来他们都在发现并报告这些漏洞。每个领先的 DNS 软件供应商都遵循普遍接受的最佳实践来处理、修复和披露软件漏洞。然而，关于用户是否以及以多快的速度将其软件更新到最新的改进版本，并没有可靠的信息来源。

一般来说，在 FOSS 中，用于评估这种风险的数据有限。软件使用者经常通过第三方（操作系统封装方，或可能已复制并重新分发软件的 FOSS 爱好者）接收软件，这一事实使得跟踪更新的部署变得更加困难。通过法规要求运营商就对其生产运营至关重要的任何软件进行某种形式的集中报告，或许可以应对这一风险。

[56] 例如，德国一家 FOSS 开发者商业协会在 FOSS 公共采购中就曾指出这一问题。请参阅开源商业联盟采购工作组发布的“开源软件可持续采购选择标准”，开源商业联盟，2025 年 2 月 11 日，https://osb-alliance.de/publikationen/veroeffentlichungen/selection-criteria-for-the-sustainable-procurement-of-open source-software。

[57] 菲利波 • 瓦尔索达 (Valsorda, Filippo)。“我现在是一名全职专业开源维护者”，2023 年 2 月 2 日。https://words.filippo.io/full-time-maintainer/。

[58] 本报告涉及的几个 FOSS 系统都有支持合同。

外包和技能短缺

正确运营 FOSS 所面临的复杂性是一个问题，因为全球部分地区缺乏技能娴熟的运维人员。这种关键性和复杂性的叠加导致一些决策者选择将业务外包给云服务，这可能会削弱系统的多样性和分布式特性，从而可能降低系统的弹性和安全性。例如，如果某个地区的所有人都选择使用一家主流的托管电邮提供商，因为这比构建、运营和维护自己的电子邮件服务器更容易，那么整个地区的电子邮件可用性就取决于这一家电邮提供商的稳定性。

此外，企业和小型服务提供商也出现了代际转变，年轻一代的员工更加依赖云服务，对自行运营网络服务不太熟悉。多家组织（例如 APNIC、NSRC、PCH）会为运营商举办培训活动，以培养他们的 DNS 和其他网络管理技能。FOSS 项目正试图通过预编译软件包和易用性功能来解决此问题，但仍难以与软件即服务替代方案竞争。

4 FOSS 在 DNS 和域名注册基础设施中的普及度

FOSS 在互联网域名和注册系统的技术运营中发挥着至关重要的主导作用。在该基础设施最关键的部分中，采用 FOSS 是常态，采用专有软件则是例外。本报告的研究表明，全球分布式 DNS 基础设施依赖于 FOSS。互联网 12 家 RSS 运营商中至少有 9 家完全采用 FOSS DNS 实现。同样，10 家最大的 TLD 服务提供商中有 9 家采用 FOSS。在域名注册领域，虽然许多大型系统是专有系统，但它们绝大多数都基于 FOSS 组件构建，而且为注册管理机构和注册服务机构提供数据托管服务的主要提供商也基于 FOSS 构建。以下几节详细介绍了 FOSS 在这一关键基础设施各个组件中的普及度。具体方法见附录 B。

4.1 域名注册基础设施中的 FOSS

注册基础设施是指用于促进单个域名注册并将已注册域名发布到公共 DNS 的系统。虽然目前尚无关于 FOSS 使用范围的明确数据，但现有证据表明，无论是作为完整的系统还是作为基础组件，对 FOSS 的依赖都已根深蒂固。

许多注册管理运行机构维护的注册基础设施完全基于 FOSS（表 1）。例如，FRED 注册管理机构平台已知至少被 12 个 ccTLD 注册管理机构使用，而 Nomulus 平台则被多个 gTLD 注册管理机构使用。

表 1：用于注册管理机构运营的 FOSS 系统

软件系统	开源许可	使用方
FRED	GPLv3	（至少）阿尔巴尼亚、安哥拉、阿根廷、波斯尼亚和黑塞哥维那、哥斯达黎加、捷克共和国、莱索托、澳门特别行政区、马拉维、北马其顿、巴拉圭和坦桑尼亚的 ccTLD 使用 FRED。
Internet ee domain registry	MIT	爱沙尼亚的 ccTLD (.ee)。
Namingo	MIT	Namingo 为 2026 年 ICANN 下一轮新 gTLD 项目而设计。
Nomulus	Apache 2.0	Google gTLD 注册管理机构，包括 .app 等。

表 2：基于 FOSS 组件构建的注册管理机构系统

注册管理机构系统/后端服务	使用中的开源组件示例	使用该系统/服务的注册管理机构
Afnic	网络服务器、数据库	20 个 TLD，包括 .fr
CIRA / SIDN / Hello Registry	数据库、网络服务器、应用程序服务器、报告、前端	6 个 ccTLD，6 个 gTLD，包括 .ca 和 .ie
CoCCA	网络服务器、应用程序服务器、数据库	56 个 ccTLD
CORE Association	网络服务器、数据库、Java 库	1 个 ccTLD，21 个 gTLD
GoDaddy Registry	数据库、应用程序服务器、报告、监控、日志记录、测试、前端、DNS	超过 200 个 TLD
Identity Digital	数据库	250 个 gTLD 和 ccTLD，包括 .au、.me 和 .pr ccTLD
Nominet	数据库、应用程序服务器、解析、日志记录、测试、前端、域名服务器	超过 85 个 TLD，包括 .uk
TANGO Registry Services	网络服务器、数据库、Java 库	8 个 gTLD
Tucows Registry	数据库、DNS 软件及配套工具、网络和邮件服务器、消息队列、基础设施编排和虚拟化、操作系统	222 个“TLD”，包括作为 TLD 管理的 SLD，例如 .my 和 com.my

注册管理机构系统/后端服务	使用中的开源组件示例	使用该系统/服务的注册管理机构
Verisign[59]	（未提供）	.com、.net、.edu 和其他 TLD

[59] Verisign 为本报告提供了以下声明：“Verisign 使用其专有的高级事务查询和分析系统 (Advanced Transaction Lookup and Analysis System, ATLAS) DNS 解析平台。Verisign 还使用专门构建的注册和解析基础设施，该基础设施采用多种精心挑选的商业和开源软件组件，以实现冗余。”

相比之下，规模最大的注册管理机构和注册管理机构后端通常使用专有系统。然而，这些系统通常不是从零开始构建的；它们通常基于对组件（如数据库和网络服务器）的专有、定制扩展和集成，而这些组件大多是 FOSS（表 2）。

对 FOSS 的这种依赖也适用于数据托管服务，这些服务安全地存储域名注册数据的副本。为注册管理机构和注册服务机构提供这些服务的三大提供商，其系统至少部分基于 FOSS 组件构建（表 3）。

表 3：数据托管代理中的 FOSS

数据托管代理	面向注册管理机构	面向注册服务机构	是否在关键功能中采用 FOSS？
北龙泽达（北京）数据科技有限公司	✓	✓	否
中国互联网络信息中心 (CNNIC)	✓	✓	否
政务和公益机构域名注册管理中心 (CONAC)	✓	✓	否
DENIC Services GmbH & Co. KG	✓	✓	是，部分
Escrow4All	✓		是
“MSK-IX”互联网交换联合股份公司	✓	✓	未知
NCC Group	✓		是，部分
中华台北网络信息中心 (TWNIC)	✓		否

本报告未对注册服务机构基础设施进行衡量或调查。我们认为，注册服务机构很可能经常使用专有、定制的组件扩展和集成，而这些组件大多是 FOSS。例如，一些注册服务机构使用 nginx 或 Apache 网络服务器软件来运营其面向注册人的网站门户。他们还使用 FOSS 解决方案来监控软件、分析数据、管理代码以及满足其他需求。

4.2 DNS 发布基础设施（权威服务器）中的 FOSS

在发布域名信息的基础设施中，FOSS 的主导地位最为明显。在 DNS 层级结构的最高层，即根和 TLD，FOSS 几乎无处不在。

RSS 是 DNS 层级结构中的最顶层。在运营根服务器的 12 家独立组织中，至少有 9 家组织完全使用 FOSS DNS 实现来回应查询（表 4）。

表 4：FOSS 在根服务器系统中的使用情况

根服务器标识符	软件	开放源[60]
A，J	ATLAS（专有） NSD	部分[61]
B	Knot BIND9	是[62,63]
C	BIND9	是
D	NSD	是
E	*未知* (FOSS)， *内部*（专有）[64]	部分[65]
F	BIND9， *内部*（专有）[66]	部分
G	BIND9	是
H	NSD	是
I	*保密*	是[67]
K	BIND9 Knot NSD	是
L	Knot NSD	是
M	BIND9	是[68]

[60] 威勒姆 • 图洛普 (Willem Toorop) 等人，“RSSAC028 实施研究报告”（报告，NLnet Labs 和 Stichting Internet Domeinregistratie Nederland (SIDN)，2023 年 9 月 27 日），第 15 页，https://www.icann.org/en/system/files/files/rssac028-implementation-study-report-27sep23-en.pdf。

[61] 摘录自 Verisign 关于 RSSAC001v2 根服务器服务期望的声明，“Verisign 使用两种不同的代码库来实现 DNS 根服务：(1) 我们专有且已获专利的 ATLAS 解析平台，以及 (2) 开放源 NLnet Labs 域名服务器守护程序 (Name Server Daemon, NSD) 软件。在任何给定时间，都可能使用其中一种或同时使用两种实现方式”，https://a.root-servers.org/aroot-rssac001v2-expectations.pdf。

[62] “USC/ISI 的 DNS 根服务器”，https://b.root-servers.org/。

[63] “RSSAC023v2：根服务器系统发展史”。ICANN 根服务器系统咨询委员会 (RSSAC)，2020 年 6 月 17 日。https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-023-17jun20-en.pdf。

[64] 丹妮 • 格兰特 (Grant, Dani)。“交付点”。Cloudflare 博客，2017 年 9 月 10 日。https://blog.cloudflare.com/f-root/。

[65] 拉尔夫 • 比肖夫 (Bischof, Ralph)。“旧金山 E 根节点出现 Servfail 错误？”，2025 年 6 月 19 日。https://lists.dns-oarc.net/pipermail/dns-operations/2025-June/022899.html。

[66] 格兰特，“交付点”。

[67] 经 Netnod 许可，摘录自其与 SSAC 于 2024 年 12 月 13 日的往来信函。

[68] “M 根 DNS 服务器”，https://m.root-servers.org/。

综合来看 ccTLD 和 gTLD 时，我们发现，在为 TLD 注册管理机构提供权威服务的前 10 家运营商中，有 9 家使用 FOSS。[69]

在根和 TLD 之下，权威域名服务器由包括个人、企业、大学和政府在内的众多实体运营。虽然没有关于这个多样化群体的全面数据，但众所周知，许多在根和 TLD 中使用的 FOSS 系统也是这些运维人员最受欢迎的选择。许多提供二级 DNS 的组织同时也为 TLD 提供权威 DNS 服务。表 5 和表 6 列出了适用于权威 DNS 实现的 FOSS 系统和商业产品。

权威域名服务器通常与置备系统集成，以便于轻松更新区信息，并对这些记录的维护实施适当的授权和控制。一些比较主流的置备系统均为 FOSS。[70]

互联网上许多最受欢迎的内容都托管在少数几个大型内容网络中，例如 Google 旗下的 YouTube，它采用专有 DNS 系统。虽然为层级结构中的二级及以下层级提供权威服务的许多大型运营商使用 FOSS（例如，同时也服务于根区或 TLD 区的运营商），但没有足够的公开声明可以可靠地调查和统计他们使用 FOSS 的情况。[71]请参阅下面的几个表格以了解更多信息。这是我们现有信息中的一个显著缺口，因为四家超大型提供商可能承载了互联网上可见权威域名查询总量的一半以上。[72]

4.3 DNS 检索基础设施（解析器）中的 FOSS

FOSS 的普及不仅限于 DNS 数据的发布；在检索这些信息的基础设施，即多样化的 DNS 解析器生态系统中，它也同样重要。FOSS 在整个解析器生态系统中占据着重要地位，从本地网络到全球云平台无处不在。

大多数用户使用的都是由其 ISP、企业或教育机构运营的本地解析器。研究估计，全球范围内使用云解析器的用户总数占比不足 20%。剩余 80% 的用户则使用某种形式的本地解析器。[73]许多最常见的 FOSS 系统可同时用于权威和解析器功能（表 5）。

[69] 运营商按所服务的 TLD 数量排名。有关所采用的方法的描述，请参阅附录 B。
[70] 主流系统包括由 Comcast 维护的 VinylDNS (https://www.vinyldns.io/) 以及由 Amazon 和 Oracle 维护的 OctoDNS。DNS Control 是另一个主流配置系统，它跨自托管系统和云服务管理 DNS，包括 Cloudflare、Amazon 的 Route53 服务以及 DNS 注册服务机构和托管提供商 Gandi。
[71] 对 FOSS 的使用情况进行可靠的衡量是一个难题。丹尼尔 • 斯坦伯格 (Daniel Stenberg) 在“我们无法衡量的事物”一文中列举了造成这种困境的几个原因，Daniel://Stenberg://（博客），2025 年 6 月 5 日，https://daniel.haxx.se/blog/2025/06/05/what-we-cant-measure/。
[72] 杰夫 • 休斯顿 (Huston, Geoff)。“审视 DNS 中的中心性”。APNIC 博客（博客），2022 年 11 月 22 日。https://blog.apnic.net/2022/11/22/looking-at-centrality-in-the-dns/。
[73] 休斯顿，“审视 DNS 中的中心性”。

表 5：用于 DNS 服务器应用的常用 FOSS 系统

软件系统	开源许可	应用 - 示例用户
BIND9	MPL 2.0	权威、解析器 - CIRA、NIC.BR、Visionary Broadband
CoreDNS	Apache 2.0	Kubernetes，权威 - Meta
dnsdist	GPL 2.0	DNS 负载均衡
Dnsmasq	GPL 2 或 3	主要为解析器 - 在嵌入式系统中很受欢迎，例如 OpenWRT、家庭网关。
Knot DNS	GPL 3.0	权威 - .cz TLD
Knot Resolver	GPL 3.0	解析器 - DNS4EU
NSD	BSD 3-Clause	权威 - Rcode Zero
PowerDNS	GPL 2.0	权威 - Rakuten
PowerDNS Recursor	GPL 2.0	解析器 - 英国电信
Unbound	BSD 3-Clause	解析器 - Quad9、Let's Encrypt
YADIFA	BSD 3-Clause	权威 - .eu TLD

虽然该市场上有许多商业产品，但其中大多数都将一个或多个 FOSS 解决方案作为其产品的核心 DNS 组件（表 6）。

在云计算领域，Microsoft Azure、Google Cloud 和 Amazon 的 AWS 等超大规模计算平台都运营着重要的解析器基础设施，以支持其服务。至少有四家最大的超大规模企业依靠 FOSS 进行 DNS 解析，[74]其他企业则在 FOSS DNS 库的基础上构建了专有解决方案（表 7）。

最后，一些终端用户会配置他们的系统，绕过网络运营商提供的解析器，转而使用开放的公共解析器。虽然两个最主流的公共服务（Google 的 8.8.8.8 和 Cloudflare 的 1.1.1.1）采用专有软件，但其他主要的公共解析器（例如 Quad9 (9.9.9.9) 和 DNS4EU）均基于 FOSS 构建。更多详情见附录 B。

[74] 出于保密原因，故意含糊其辞。

表 6：使用 FOSS 的商业 DNS 服务示例

制造商	产品	应用	使用 FOSS
Akamai	Edge DNS	混合云解析器和权威服务	否
Bluecat Networks	Integrity、Micetro	权威、解析器	是
Cygna Labs	VitalQIP、DiamondIP	权威、解析器	是
EfficientIP	SolidServer DDI	权威、解析器、设备和云	是
F5	BIG-IP DNS	解析器	是
IBM	NS1 Connect	基于云的权威服务	未知
InfoBlox	Universal DDI & NIOS DDI	权威、解析器、设备和云	是
Knipp	IronDNS	权威	部分
Microsoft	Windows Server DNS	权威、解析器，用于企业网络，与 Active Directory 集成	否
	Azure DNS	云解析器服务	是
Netgate	pfSense	解析器	是
Oracle	OCI DNS	权威云服务	是
TCPWave	DDI Management	权威设备	是

表 7：用于 DNS 基础设施应用的 FOSS 库

软件系统	编程语言	应用 - 示例用户
c-ares	C	libcurl、curl、NodeJS
dnsjava	Java	（专有）注册管理机构后端
dnspython	Python	Mailman、Samba、Ansible
domain	Rust	Cascade
miekg/dns	Go	Let's Encrypt、CoreDNS、Docker
ldns	C	Zonemaster、dnstap、（专有）域名服务器
libunbound	C	Open vSwitch、libreswan、opendkim
Net::DNS	Perl	Spamassassin、Mail::DMARC、Mail::DKIM、Mail:SPF

5 FOSS 监管领域的当代案例

本节考察了美国、英国和欧盟的几个当代案例，这些案例说明了政策制定者如何调整网络安全法规，以适应 FOSS 生态系统的独特现实。表 8 简要汇总了这些方法。这些方法体现了一种模式，即免除志愿维护者的直接责任，同时重点关注集成或部署 FOSS 的商业实体的责任。接下来将详细探讨每个案例。

表 8：FOSS 当代监管方法汇总

章节	核心关注点	示例法规	FOSS 处理方式
5.1	分配责任	2023 年美国网络安全战略，2025 年英国准则	免除维护者责任，重点关注商业实体
5.2	激励合作	欧盟网络弹性法案	引入可选的“管理者”角色，以激励提供支持
5.3	避免专有假设	欧盟 NIS 2 实施法案	无合同 = 无直接供应商，鼓励提供支持
5.4	避免制度冲突	欧盟 NIS 2 指令	避免根服务器等全球要素的重叠

5.1 向最有行动能力的利益相关方分配责任

2023 年美国国家网络安全战略[75]寻求转移不安全软件产品和服务的责任归属（战略宗旨 3.3）。该战略制定了一个高层次的愿景，即“制造软件的公司必须拥有创新的自由，但当他们未能履行对消费者、企业或关键基础设施提供商的审慎义务时，也必须承担责任”。从一开始，该战略对 FOSS 维护者采取了更细化的差异化处理：“责任应归于最有能力采取行动避免不良后果的利益相关方，而非常为不安全软件承担后果的终端用户，亦非被集成至商业产品中的组件的开源开发者。”

同样，英国的 2025 年《自愿性软件安全实践准则》[76]旨在“支持软件供应商及其客户减少软件供应链攻击和其他软件弹性事件的可能性和影响”。它同样适用于商业软件供应商：“对于开源软件，开发者/维护者对其后续供应链或其代码的持续维护和安全不负有任何正式责任。与开源代码相关的任何风险都必须由终端用户或在其软件中使用开源代码的专有开发人员负责。”

[75] 美国总统。“国家网络安全战略”。华盛顿特区：白宫，2023 年 3 月 1 日。https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf。
[76] “软件安全实践准则”。

5.2 推动全行业协作，实现可持续维护

欧盟 CRA[77] 旨在解决“具有数字元素的产品网络安全级别较低的问题，这体现在普遍存在漏洞，以及为解决这些漏洞而提供的安全更新不足且不一致”。在同样豁免未将 FOSS 商业化的 FOSS 维护者责任的同时，它通过引入一个新的法律主体（“开源软件管理者”）来激励跨行业合作，以促进 FOSS 的可持续维护，该角色需“为软件开发提供持续支持”，并确保“这些产品的可行性”。管理者是一种可选且尚未普及的组织角色，FOSS 维护者可以选择与之建立联系，作为从依赖于 FOSS 的重要基础设施制造商或运营商那里输送资源的一种手段。虽然目前由类似管理者的组织提供支持的 FOSS 数量很少，但 CRA 今后可能会增加这种做法，而且它很可能适用于一些维护 DNS 软件的组织。最后一项监管创新是未来可选择“自愿安全认证”，允许跨行业合作开展尽职调查。

5.3 避免默认采用专有软件模式的供应链安全要求

欧盟 NIS 2 指令旨在“缓和对用于提供关键领域基本服务的网络和信息系统的威胁”。[78] 该指令将数字基础设施作为“高度关键领域”进行管理，指定了网络安全的管理责任，并规定了“风险管理措施”，这在实施法案中作了详细说明。[79]其中包含“供应链安全，包括涉及每个实体与其直接供应商或服务提供商之间关系的安全相关方面”。规定这些要求的附件源自 ISO/IEC 27002:2022 中的控制措施，但它假定了贯穿至软件开发者的合同义务链，这与 FOSS 的实际情况（参阅第 3.2.2 节）并不相符。

欧盟网络安全局在其针对受监管实体的技术实施指南[80]中，澄清了有关 FOSS 的“直接供应商和服务提供商”概念：“就自由与开放源码软件 (FOSS) 而言，如果相关实体与开源项目之间不存在合同关系（除了遵守标准化版权许可之外），或者与开源软件管理者存在合同关系，则公开开发、维护和分发软件的社群和项目可能不会被视为直接供应商或服务提供商。”其建议是：“考虑为开发和维护 FOSS 的社群提供支持，并加大投入，与他们建立互利共赢的关系。如果有效的话，这可能涉及与相关 OSS 管理者建立关系，OSS 管理者‘为软件开发提供持续支持，并确保这些产品的可行性’。”

[77] 欧洲议会和欧盟理事会 2024 年 10 月 23 日关于具有数字元素产品的横向网络安全要求的第 (EU) 2024/2847 号条例，修订了第 (EU) 168/2013 号和第 (EU) 2019/1020 号条例以及第 (EU) 2020/1828 号指令（网络弹性法案），2024 O.J. (L 2024/2847) 1，https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng。
[78] 欧洲议会和欧盟理事会 2022 年 12 月 14 日关于在欧盟范围内实现高水平网络安全统一措施的第 (EU) 2022/2555 号指令（NIS 2 指令），2022 O.J. (L 333) 80，https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng。
[79] 欧盟委员会第 (EU) 2024/2690 号实施条例，2024 年 10 月 22 日通过，旨在制定欧洲议会和欧盟理事会第 (EU) 2024/2847 号条例的实施细则，2024 O.J. (L 2024/2690) 1，https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj。
[80] 欧盟网络安全局 (European Union Agency for Cybersecurity, ENISA)，NIS2 技术实施指南（报告，欧盟出版办公室，2025 年），https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance。

英国科学、创新和技术部委托编写的 2025 年报告调查了开源和供应链风险的行业实践。[81]其中，该报告建议组织“制定内部 OSS 政策来管理 OSS 组件的采用”，并“促进与 OSS 社群的积极合作，以确保高质量的 OSS 组件和可持续的 OSS 生态系统”。与此相反，不适合 FOSS 的供应链安全条例会向运营商施加合同义务，要求其对 FOSS 维护者进行背景调查，认为他们是“供应商”，即使 FOSS 并非通过购买获得。这种考虑不周的法规可能会导致 FOSS 技术人员放弃他们的项目，使项目的维护者人数减少或能力降低，从而导致质量下降。这与供应链安全监管的预期效果背道而驰。

5.4 避免针对全球 FOSS 社群的地区制度冲突

对软件开发及其在关键基础设施中的使用进行直接监管的做法并不普遍。由于 FOSS 允许全球合作开发（第 3.2.1 节），未来的监管制度应避免因个别维护者的实际所在地不同而产生重叠和相互冲突的要求。

上文提到的欧盟 NIS 2 指令[82]在对 DNS 服务提供商的要求中，非常注意避免出现类似的制度重叠情况，该指令将根域名服务器排除在监管范围之外，从而避免了根服务器运营商遭遇地区制度重叠、有时甚至相互冲突的情况。[83]

6 主要结论

本节将报告的核心分析汇总为一系列结论，为后续的可行指导方针提供证据基础。

结论 1：FOSS 是关键 DNS 基础设施的基础。全球的政策制定者和监管机构都在努力确保软件供应链的安全，因此，在开展这些工作时，务必要清晰理解互联网最基础系统的实际构建和维护方式。本报告的研究表明，当今全球 DNS 基础设施绝大部分依赖于 FOSS。在该基础设施最关键的部分中，采用 FOSS 是常态，采用专有软件则是例外。这包括 RSS（12 家运营商中至少有 9 家完全使用 FOSS DNS 实现）和 TLD（10 家最大的服务提供商中有 9 家使用 FOSS）。

结论 2：FOSS 的开发模式与专有软件有着根本的不同。专有软件通常由一个组织在内部创建，而 FOSS 的模式是开放且分布式的。它建立在其许可证所赋予的四项基本自由之上：自由使用、自由研究、自由分享和自由修改软件。这种框架形成了一个由维护者、贡献者和运营商组成的独特生态系统，他们通常不受传统商业供应链中合同关系的约束。

[81] “开源软件最佳实践与供应链风险管理”。
[82] NIS 2 指令。
[83] 伯特・休伯特 (Bert Hubert) 的观点摘要见“尊敬的欧盟：请不要破坏根”，2021 年 5 月 10 日，https://berthub.eu/articles/posts/dont-ruin-the-root/。

结论 3：FOSS 本质上并不比专有软件更安全或更不安全；安全性取决于流程和维护，而不是源代码的可见性。这种开放模式对安全的影响必须结合几十年来一直没有明确答案的争论问题来理解。正如安全工程研究员罗斯·安德森 (Ross Anderson) 所总结的，对于大型复杂系统来说，源代码的可见性对攻击者和防御者的帮助是均等的。从长远来看，一个系统是开放的还是封闭的，对其安全性没有多大影响。隐藏源代码并不能提供额外的安全性；系统的安全性而是来自于其开发、审核和维护流程的质量。

结论 4：DNS FOSS 生态系统具有独特的优势，可提高稳定性和弹性。虽然开放性本身可能是中立的，但它所促成的合作过程对于建设和维护关键互联网基础设施特别有效。FOSS 固有的透明度使全球的开发人员、研究人员和运维人员能够研究源代码并共同解决漏洞，这种做法往往比专有系统更快地修补漏洞。这就带来了固有的优势，包括增强的合作安全性、软件多样性带来的运营弹性，以及由专注的非营利组织和商业组织提供的长期支持所带来的卓越稳定性。

结论 5：FOSS 模式有其固有风险，需要采取量身定制而非“一刀切”的政策方法。提供这些优势的特性同样也带来了一系列特有的风险，需要采取量身定制的政策方法。由于 FOSS 的开发模式使资金与使用脱钩，项目可能面临资金可持续性和维护者职业倦怠方面的挑战，在这种情况下，关键基础设施可能依赖于少数人在无资金支持下的自愿付出。此外，FOSS 组件的广泛复用也带来了共享型依赖关系风险，即单个库中的漏洞可能会在整个生态系统范围内产生连带影响。这些问题无法通过为商业专有软件市场制定的法规来解决。

结论 6：为 FOSS 的开发与分发附加新的法律和财务责任时，必须审慎行事，以免破坏催生出这一互联网基础设施根本要素的生态环境。由于 FOSS 项目缺乏单一责任法律实体或传统的合同链，因此采用传统的责任框架既不现实，也存在风险。FOSS 的开发模式依赖于个人志愿者和资金极少的小型组织。对这些维护者施加沉重的监管负担，可能会打压他们的参与积极性，从而有可能扼杀创新想法，并最终导致对关键互联网基础设施至关重要的软件被弃用。

结论 7：FOSS 对于新提供商进入互联网服务市场非常重要，也为政策制定者提供了机会来鼓励开发本地服务并减少对外国云计算提供商的依赖。除了技术方面的作用之外，FOSS 还能推动经济增长、数字自主和市场竞争。FOSS 开发模式通过取消软件许可费，降低了新企业进入市场的成本。这种可及性促进了本地创新和技能发展，为政策制定者提供了一种有效途径来打造更加多样化的数字生态系统，并有助于减少对外国云服务的依赖。

7 面向政策制定者的可行指导方针

本节基于报告的结论，为政策制定者提供直接、可行的指导方针。其目标是，制定有效且无负面影响的法规，以加强而非削弱对互联网安全稳定运行至关重要的 FOSS 生态系统。

指导方针 1：认可 FOSS 的关键作用。本报告证实了全球 DNS 基础设施依赖于 FOSS。在该基础设施最关键的部分中，采用 FOSS 是常态，采用专有软件则是例外。因此，政策制定者应在任何相关立法或法规中明确认可，FOSS 是关键互联网基础设施的基础，并且其使用是一种应予以保持和巩固的优势。这种认可应该从最初的设计阶段开始就告知监管机构，以防止对生态系统造成意外损害。

指导方针 2：咨询 FOSS 社群。FOSS 的开发模式是开放且分布式的，与专有软件有着根本的不同。它是一个由维护者、贡献者和运营商组成的生态系统，他们通常不受传统商业供应链中合同关系的约束。在整个政策制定流程中，必须让 FOSS 生态系统的所有各方（包括公司、非营利组织、个人维护者和社群机构）参与进来。这能确保法规的制定充分考量他们的实际运营状况，从而防止对 FOSS 生态系统乃至关键互联网基础设施造成意外损害。

指导方针 3：借鉴 FOSS 监管领域的当代案例。正如第 5 节所述，近期的一些监管措施已经开始着手应对 FOSS 的独特特性，同时仍在推进重要的政策目标。这些案例为制定符合 FOSS 生态系统独特特性的新政策提供了宝贵的框架。借鉴这些经验意味着设计的政策和法规符合以下要求：

- 将责任分配给最有能力采取行动的利益相关方。审慎义务应由在商业产品或关键基础设施中部署软件的实体承担，而不是由创建组件的 FOSS 志愿开发者承担。
- 激励可持续维护方面的跨行业合作。可以通过支持创新型法律模式（例如引入“开源软件管理者”）来确保关键 FOSS 产品的可行性，这些模式可以从行业输送资源。
- 避免假设专有软件模式的供应链安全要求。请记住，在 FOSS 领域，维护者和运营商之间通常除了开源许可本身之外，没有直接的合同关系。
- 避免全球 FOSS 社群的地区制度发生冲突。应在法规中避免全球 FOSS 项目的义务重叠和矛盾，以防止开发工作的碎片化与安全性的削弱。

指导方针 4：激励 FOSS 可持续发展。FOSS 模式使资金与使用脱钩，众所周知，这会导致财务可持续性挑战和维护者职业倦怠。关键基础设施可能依赖于小型组织，或少数人在无资金支持下的自愿付出。为缓和这种风险，建议政策制定者制定有利的政策，鼓励公共和私营部门为关键 FOSS 项目做出贡献，以此作为对共享公共利益的投资形式。

指导方针 5：共同应对系统性风险。FOSS 组件的广泛复用也带来了共享型依赖关系风险，即单个库中的漏洞可能会在整个生态系统范围内对 FOSS 和专有软件产品产生连带影

响。由于这是所有现代软件开发所固有的系统性风险，政策应促进并资助整个生态系统范围的合作解决方案，如改进的安全工具和独立研究，而不是将全部负担压在个别志愿维护者身上。

8 致谢、利益披露和回避

为了确保公开透明，以下部分为读者提供了有关 SSAC 流程方面的信息。“致谢”部分列出了作为共同作者或直接参与本文档撰写或提供审阅意见的 SSAC 成员、外部专家和 ICANN 员工。“利益披露”部分提供了所有 SSAC 成员的个人简介链接，其中包含对可能与成员参与本报告准备工作产生冲突（真实、明显或潜在冲突）的任何利益披露。“回避”部分列出了要求不参与本报告中所涉及主题讨论的个人成员。本文档已得到除“回避”部分中列出的成员之外的所有 SSAC 成员的一致批准。

8.1 致谢

委员会感谢以下 SSAC 成员、特邀人员和 ICANN 员工花费时间来撰写和审查本报告。

SSAC 成员
乔・阿布力 (Joe Abley)
马丁・阿特森（Maarten Aertsen，工作组联合主席）
高塔姆・阿基瓦特 (Gautam Akiwate)
蒂姆・阿普利 (Tim April)
纳比尔・博纳玛 (Nabil Benamar)
KC・珂拉菲 (KC Claffy)
哈迪亚・埃米尼维 (Hadia Elminiawi)
安德雷・菲利普（Ondrej Filip，SSAC 成员，至 2024 年 12 月 31 日）
詹姆斯・加尔文 (James Galvin)
罗伯特・盖尔拉 (Robert Guerra)
鲁斯・胡斯利 (Russ Housley)
马蒂亚斯・胡多布尼克 (Matthias Hudobnik)
吉奥夫・休斯顿 (Geoff Huston)
莱亚尔・杰布兰 (Layal Jebran)
梅丽克・凯奥（Merike Kaeo，SSAC 成员，至 2024 年 12 月 31 日）
安德烈・克莱斯尼科夫 (Andrei Kolesnikov)
沃伦・艾斯・库马里 (Warren “Ace” Kumari)
巴瑞・莱巴（Barry Leiba，工作组联合主席）
约翰・莱文 (John Levine)
拉斯・芒迪 (Russ Mundy)
拉姆・莫罕 (Ram Mohan)
马特・托马斯 (Matt Thomas)
彼得・托玛森 (Peter Thomassen)

塔拉・瓦伦 (Tara Whalen)
苏珊・沃尔夫 (Suzanne Woolf)
姚健康 (Jiankang Yao)

特邀人员
维托里奥・博托拉 (Vittorio Bertola)
梅丽克・凯奥（Merike Kaeo，2025 年 1 月 1 日起作为特邀人员）
维姬・里斯克 (Vicky Risk)
拉斐尔・索梅塞 (Raffaele Sommese)

ICANN 员工
约翰・埃默里（John Emery，编辑）
丹尼尔・格鲁克 (Daniel Gluck)
古斯塔夫・洛赞诺・伊巴拉 (Gustavo Lozano Ibarra)
迈克尔・普基特 (Michael Puckett)
卡洛斯・雷耶斯 (Carlos Reyes)
丹妮尔・卢瑟福特（Danielle Rutherford，编辑、特约撰稿人）
凯西・什尼特 (Kathy Schnitt)
史蒂夫・盛（Steve Sheng，SSAC 支持人员，至 2024 年 11 月 30 日）

8.2 利益披露

SSAC 成员个人简介和本文发布时的利益披露详见：
https://www.icann.org/en/ssac/members/archive/16-05-2025。

8.3 回避声明

无回避情况。

附录 A：术语表和缩略语

A.1 术语表

权威服务器：用于保存特定域名的权威、官方 DNS 记录的服务器。它提供该域名 DNS 查询的最终答案。

贡献者：提供 FOSS 项目改进方案的个人或组织，如提交代码、文档或错误报告。

数据托管：将域名注册数据的副本存储在 ICANN 认证第三方，以妥善保管。

域名：唯一且人类可读的名称（例如 icann.org），用于标识互联网上的特定地址，是构成 URL 的基础。

域名系统 (Domain Name System, DNS)：作为“互联网地址簿”的全球去中心化系统，将人类可读的域名转换为定位计算机服务和设备所需的数字 IP 地址。

可扩展供应协议 (Extensible Provisioning Protocol, EPP)：标准化技术协议，用于在域名注册服务机构和注册管理机构之间自动进行交易，如注册、续订和转让。

分支：通过从现有 FOSS 项目中复制源代码而启动的新的独立软件项目。

自由与开放源码软件 (Free and Open Source Software, FOSS)：软件的许可方式赋予用户四项基本自由：自由使用、自由研究、自由分享和自由修改软件。这定义了一种合作开发模式，而不仅仅是免费软件。

互联网协议 (Internet Protocol, IP) 地址：为与使用互联网协议进行通信的计算机网络连接的每台设备分配的唯一数字标签。

国际化域名 (Internationalized Domain Name, IDN)：一种域名，其中有一个或多个标签包含了除美国信息交换标准码 (ASCII) 字母、数字或连字符之外的其他字符。

维护者：负责 FOSS 项目整体方向和质量控制的个人或团体。他们有权接受或拒绝他人对软件官方版本的贡献内容。

运营商：部署和使用软件以运行服务的个人或组织。在 DNS 的语境下，“运营商”是指运行 DNS 基础设施组件（如权威服务器或解析器）的实体。

发布（在 DNS 中）：将域名的 DNS 记录放置到权威服务器上，以便其他人能在互联网上找到该域名的技术过程。

递归解析器（或解析器）：通常由互联网服务提供商 (ISP) 运营的服务器，代表用户的设备为请求的域名查找正确的 IP 地址。

注册（在 DNS 中）：通过将域名添加到特定顶级域的权威主数据库（注册管理机构）来保留唯一域名的管理过程。

注册人：注册并拥有特定域名所有权的个人或组织。

注册服务机构：面向公众的组织，充当域名零售商，代表注册人管理域名留存事宜。

注册管理机构：权威主数据库，其中包含在特定顶级域（如 .org 注册管理机构）内注册的所有域名。维护此数据库的组织为注册管理运行机构。

根服务器系统 (Root Server System, RSS)：DNS 层级结构中最高层的服务器集合，负责将查询定向到正确的顶级域服务器。

顶级域 (Top-Level Domain, TLD)：位于最后一个点右侧的域名部分，例如 .com、.org 或 .uk。

统一资源定位符 (Uniform Resource Locator, URL)：用于在互联网上查找特定资源的完整地址，通常包括协议（例如 https）、域名和具体路径（例如 https://www.icann.org/resources）。

A.2 本报告中使用的缩略语

ccTLD：Country-Code Top-Level Domain（国家和地区顶级域）
DNS：Domain Name System（域名系统）
EPP：Extensible Provisioning Protocol（可扩展供应协议）
FOSS：Free and Open Source Software（自由与开放源码软件）
gTLD：Generic Top-Level Domain（通用顶级域）
IP：Internet Protocol（互联网协议）
ISP：Internet Service Provider（互联网服务提供商）
RSS：Root Server System（根服务器系统）
SSAC：Security and Stability Advisory Committee（安全与稳定咨询委员会）
TLD：Top-Level Domain（顶级域）
URL：Uniform Resource Locator（统一资源定位符）
IDN：Internationalized Domain Name（国际化域名）

附录 B：FOSS 普及度研究方法和结论

本附录提供了该报告原始研究的完整、独立的摘要。其中详细介绍了用于获取自由与开放源码软件 (FOSS) 普及度研究结论的方法以及研究结论本身，相关结论在本报告第 4 节中进行了说明。

B.1 一般方法和挑战

要确切查明软件运营商在实际环境中使用何种软件，是一项颇具挑战性的任务。虽然引入了某些域名系统 (DNS) 记录（如 version.bind、authors.bind、id.server）来帮助终端用户识别与之通信的 DNS 服务器版本，但由于存在潜在安全风险且需要手动配置，这些记录并未获得广泛采用。文献中还探讨了其他方法，包括被动分析和主动衡量。不过，这些方法的范围往往有限，有些只能识别递归基础设施，而且在可扩展性方面也面临挑战。

出于这些原因，本报告采用的方法主要是按市场份额对大型 DNS 运营商进行评估，因为对于这些运营商，可以明确证实其大量使用了开源软件。

B.2 域名注册基础设施

B.2.1 方法

为评估 FOSS 在注册基础设施中的使用情况，安全与稳定咨询委员会 (SSAC) 对大型注册管理机构和注册管理机构后端提供商进行了调查。为评估 FOSS 在数据托管服务中的使用情况，对 ICANN 网站上列出的 ICANN 批准的数据托管代理 (Data Escrow Agent, DEA) 进行了调查，其中重点关注用于关键服务组件（数据传输、签名验证、寄存验证以及与注册报告接口 (Registration Reporting Interface, RRI) API 的交互）的软件。

B.2.2 结论

注册基础设施是指用于促进单个域名注册并将已注册域名发布到公共 DNS 的系统。虽然目前尚无关于 FOSS 使用范围的明确数据，但现有证据表明，无论是作为完整的系统还是作为基础组件，对 FOSS 的依赖都已根深蒂固。

许多注册管理运行机构，尤其是在国家和地区顶级域 (ccTLD) 领域，都维护着完全基于 FOSS 的注册基础设施（表 1、表 2）。例如，FRED 注册管理机构平台已知至少被 12 个 ccTLD 注册管理机构使用，而 Nomulus 平台则用于多个通用 TLD (gTLD)。

相比之下，规模最大的注册管理机构和注册管理机构后端服务提供商通常使用专有系统。然而，这些系统通常不是从零开始构建的；它们是组件（如数据库和网络服务器）的专有、定制扩展和集成，而这些组件大多是 FOSS。

对 FOSS 的这种依赖也扩展到数据托管服务（表 3），这些服务安全地存储域名注册数据的副本。为注册管理机构和注册服务机构提供这些服务的大型提供商，其系统至少部分基于 FOSS 组件构建。

B.3 DNS 基础设施

B.3.1 方法

权威服务器分析：为了调查 FOSS 在 TLD 基础设施中的使用情况，我们采用了以下程序：

1. 从 IANA 获取了根区，并将 TLD 映射到其域名服务器的互联网协议 (IP) 地址。
2. 通过对双字母 TLD 及其 A-标签（国际化域名编码 (Punycode)）等效形式（用于涵盖国际化域名 (IDN) ccTLD）的综合考量，对 ccTLD 进行了单独分析。
3. Python ip2asn 库用于将这些 IP 地址映射到各自的自治系统编号 (Autonomous System Number, ASN) 和 ASN 名称（运营商）。
4. 市场份额的计算方法是：特定运营商托管的 TLD 数量除以 TLD 总数（请注意，一个 TLD 可以同时由多家运营商托管）。
5. 确定了排名前 25 位的运营商，并对他们使用开源权威域名服务器软件的情况进行了人工验证。

解析器分析：目前还没有对已安装的全部解析器进行可靠的调查。本报告的分析重点是列举主要运营商和部署类型（如本地、云端、公共），并根据公开声明和直接了解到的情况调查他们使用的是 FOSS 还是专有软件。

B.3.2 结论

权威服务器：在发布域名信息的基础设施中，FOSS 的主导地位最为明显。在 DNS 层级结构的最高层，即根和 TLD，FOSS 几乎无处不在。根服务器系统 (RSS) 位于 DNS 的顶层。在运营根服务器的 12 家独立组织中，至少有 9 家组织完全使用 FOSS DNS 实现来回应查询（表 4）。

这种模式在 TLD 域名服务器层级架构的下一层继续存在（表 5）。本报告研究发现，在为 TLD 注册管理机构提供权威 DNS 服务的前 10 家运营商中，有 9 家使用 FOSS。此

外，在为 ccTLD 提供这类服务的前 25 家运营商中，有 20 家使用 FOSS DNS 软件，总共为 234 个不同 ccTLD 提供服务。

解析器：FOSS 的普及不仅限于 DNS 数据的发布；在检索这些信息的基础设施，即多样化的 DNS 解析器生态系统中，它也同样重要。

大多数用户使用的都是由其互联网服务提供商 (ISP)、企业或教育机构运营的本地解析器。虽然该市场上有许多商业产品，但其中大多数都将一个或多个 FOSS 解决方案作为其产品的核心 DNS 组件。

在云计算领域，Microsoft Azure、Google Cloud 和 Amazon Web Services 等超大规模计算平台都运营着重要的解析器基础设施，以支持其服务。至少有四家最大的超大规模企业依靠 FOSS 进行 DNS 解析，其他企业则在 FOSS DNS 库的基础上构建了专有解决方案。

附录 C：DNS 运营商对 FOSS 和软件监管的看法调查

安全与稳定咨询委员会 (SSAC) 开展了一项非正式的在线调查，旨在了解开源软件监管对域名系统 (DNS) 基础设施的预期影响，从而为本报告收集相关意见。本次调查采用 EUSurvey 工具，以保护受访者的隐私，实现匿名性。[84]调查通过多个电子邮件清单向 DNS 技术社群征求回复，包括：欧洲国家顶级域注册管理机构理事会 (Council of European National Top-Level Domain Registries, CENTR) 的技术和法律电子邮件清单、欧洲网络协调中心 (Réseaux IP Européens Network Coordination Centre, RIPE NCC) 的 DNS 和开源工作组，以及多个开源 DNS 软件系统的用户电子邮件清单。域名系统运营、分析和研究中心 (DNS-OARC) 在 2 月份召开的会议上也对本次调查进行了介绍。

本次调查的主要目的是，了解 DNS 技术运营商是否知晓相关监管举措，并询问他们预计自由与开放源码软件 (FOSS) 监管会带来何种影响。调查于 2025 年 2 月开放。共收到 98 份回复，涵盖了 DNS 基础设施中的各类角色。

我们首先询问了受访者参与 DNS 的情况。在 98 位受访者中，有 96 位表示参与了 DNS 基础设施，另外有 64 位表示参与了域名注册基础设施。有 24 位受访者将“软件开发商/供应商”作为其角色之一，但其中没有任何受访者仅以软件开发商的身份作答。（我们没有询问他们的软件是开源还是闭源）。

受访者都是开源软件用户，而且对监管措施非常了解。几乎所有受访者都表示使用开源软件 (93%)。约有三分之一 (33%) 的受访者表示同时也使用专有软件。30% 的受访者还就 FOSS 的实施和运维向他人提供建议。这部分人对现行监管举措的认知度很高。我们提供了一份监管举措清单，并询问“您知晓其中哪些监管举措？（请勾选所有您知晓的举措）”。有 77 位受访者（约 77%）表示知晓其中一项或多项。超过 40% 的受访者熟悉欧盟网络弹性法案、网络安全法案和 NIS2。30% 的受访者表示还熟悉一项或多项美国政府倡议，包括第 14028 号和第 14144 号行政令、安全软件开发认证计划或物联网 (IoT) 设备网络信任标志。受访者提到的其他法规包括：澳大利亚关键基础设施安全法 (Security of Critical Infrastructure Act, SOCI)、通用数据保护条例 (General Data Protection Regulation, GDPR)、支付卡行业数据安全标准 (Payment Card Industry Data Security Standard, PCI DSS)，以及美国和加拿大联邦风险与授权管理计划 (Federal Risk and Authorization Management Program, FedRAMP) 授权。

我们询问“关于软件监管对贵组织的影响，您有哪些具体担忧？”，并提供了积极和消极的选项。所有受访者都能回答这个问题，包括那些并未表示熟悉我们提到的任何具体法规的受访者。

[84] “EUSurvey - 简介”。https://ec.europa.eu/eusurvey/home/about。

- 72% 的受访者认为，一些开源项目有可能被放弃或变得不可用，这种情况是相当可能发生的
- 66% 的受访者认为，合规会增加他们的软件成本
- 49% 的受访者担心，他们所依赖的一些开源项目可能会转向专有许可方式
- 29% 的受访者认为，法规会阻碍他们的组织发布开源软件
- 21% 的受访者预计，他们所用的开源软件的安全性会得以提高
- 7% 的受访者预计，法规将减轻其组织在评估软件安全性和质量方面的负担。

尽管我们特别征询了有关积极影响和机遇的意见，试图保持一种平衡的立场，但受访者大多持悲观态度。

C.1 开放式意见（具体担忧）

本调查邀请受访者就对软件监管影响的具体担忧发表开放式意见，并询问预期的机遇或积极影响。

最常提及的担忧包括：

- 合规成本增加
- 软件部署速度减慢
- 由于监管负担，一些开源项目可能被放弃
- 开源软件用户面临的法律合规复杂性增加