4. Focused Research (3)

30 Years of IIJ and DNS

4.1 Introduction

IIJ was the first commercial service in Japan to provide Internet access, something previously limited to academic institutions. That was in November 1993. This year marks 30 years since. In this chapter, we look back over the past 30 years with an eye on DNS..

4.2 1990s: Working with Connectivity Services

■ No DNS

IIJ was established in December 1992 as Internet Initiative Planning Inc., subsequently taking on its current name the following May. In July 1993, it launched the UUCP Service, and then in November, it launched its Internet Connectivity Service, Japan's first commercial Internet connectivity service.

DNS is a service that uses host names to look up IP addresses and is essential for using the Internet. It is therefore common for a caching DNS server to be bundled in when you subscribe to a connectivity service. That's par for the course these days, so you might think that IIJ's history with DNS started back when it launched its first service, but that was not the case. We only provided connectivity services via dedicated lines. A caching DNS server was not included.

Although ours was Japan's first service, most of our users were familiar with the Internet as an academic network. The Internet is a decentralized or distributed system, as opposed to a centralized one. The participants are equals, and they either arrange what they need themselves, or help each other out in the spirit of mutual aid when things are lacking. This seems to have been the common understanding among IIJ and its users. IIJ's position was that it provides everything to get you connected to the Internet, and that you are on your own from there in terms of arranging DNS, email, and online news. And the users seem to have regarded this as normal.

■ The first DNS servers

Caching DNS servers were first made available to users in May 1994 with the Dialup IP Service. This did not provide a permanent connection over a dedicated line. Instead, users connected via a phone line only when they needed to, making the service accessible to small businesses and individuals as well. Tele-Hodai, NTT's nighttime flat-rate phone service, had not yet been launched (it appeared in 1995), so the service was used in much the same manner as people used the traditional dialup online services that were popular at the time—that is, they would connect, obtain the information they needed, and then immediately disconnect. Unlike with dedicated line connections, this mode of use does not really fit with the idea of users arranging the necessary servers, and so IIJ ended up providing caching DNS in this case.

Even after IIJ started providing caching DNS servers, its position that users should arrange their own authoritative DNS server did not change. Even so, per the textbook description of DNS, you need two servers, the primary and the secondary, and it was not easy back then for users to furnish both, so there were cases in which IIJ looked after the secondary. And this seems to have been done as part of the mutual aid that Internet users provided to each other as equals, rather than for business motives. If you can believe it, the secondary DNS zone was stored on a Dialup IP Service caching DNS server. While this is unthinkable by today's standards, things were small in scale at the time, and so it was deemed reasonable to share resources.

JP domains were an important aspect when it came to secondary DNS being operated in the spirit of mutual aid. A document giving background to IIJ's involvement is even still available via JPNIC[*1].

In 1994, IIJ took on the role of JP domain secondary, and it has been doing this ever since. Its efforts since then have gone beyond mere assistance among peers. To help with the stable operation of JP domains, it has actively incorporated advanced functionality, which has included providing early support for IPv6 in 2001 and establishing an overseas presence and providing support for anycast.

■ Rise of the Internet

The mid-1990s was when the Internet started to become more accessible to individual consumers. INTERNET

[*1] JPNIC, "Report on DNS Management Group's activities (including some background on agenda items)" (https://www.nic.ad.jp/ja/materials/committee/1994/0510/shiryou-2-4-1.html, in Japanese).

magazine was first published by Impress in September 1994, and Windows 95 with TCP/IP as standard was released in Japan in November 1995. Many other ISPs beyond IIJ began to pop up around this time.

IIJ4U was launched in December 1996 to serve demand for personal Internet connectivity. The equipment was designed specifically for large-scale consumer services, and this was the first time that IIJ put two caching DNS servers on different network segments to ensure availability, something that is commonplace nowadays.

Around that time, IIJ also started providing caching DNS servers as part of its business connectivity services, but the basic approach of the customer being responsible for building and operating the servers themselves remained unchanged, so the idea was that IIJ would provide the servers only when the customer was absolutely unable to. It was in November 1997 when the IIJ Economy service made them standard.

The term SOHO has perhaps faded out of the popular vernacular somewhat by now. Short for small office / home office, it refers to the concept of using a home or a small office as your workplace. IIJ Economy was a low-cost leased line service for the SOHO market, and unlike with its traditional business connectivity services, IIJ did not expect users to set up and operate their own servers. That is, with this service, IIJ would arrange the caching DNS servers.

That is how the foundations of caching DNS services were established. IIJ subsequently released all sorts of connectivity services, including ADSL, optical fiber, VPNs, and mobile, but even with these changes in line types, the basics of caching DNS remained unchanged, albeit with enhancements to facilities and equipment.

4.3 2000s: Launch of DNS-only Services

The year 1999 saw a huge run-up in US stock market prices centered on Internet-based businesses, and even companies with nothing to do with the Internet saw their stock prices double simply after renaming to include .com in their names[*2]. The extraordinary market highs ended with the crash of 2001, and the episode is now remembered as the dot-com bubble.

With Japan remaining plagued by the Heisei Recession and the Employment Ice Age following the collapse of its bubble economy in 1991, it did not see a dot-com bubble like the US. Yet many of the companies experiencing significant growth during this era had a connection to IT, one such example being SoftBank, which saw its market cap expand to the point that it was second only to Toyota Motor.

While the stock price bubble was only temporary, the practice of companies owning their own domains was here to stay. This became commonplace at businesses across the board, not just major corporations and Internet-related names. Even if you buy a domain, you still can’t use it unless you register it with an authoritative DNS. IIJ’s stance up to this point had been that customers should handle their authoritative DNS themselves if they needed it, but that required quite a bit of expertise. The era of the Internet only being for those few people who “got it” was already over by this point, and there was rising demand for registering information on the authoritative DNS system even among people with no expertise in server operations.

In response, IIJ launched DNS-only services in March 2000: the DNS Outsourcing Service, which enabled overall authoritative DNS operations and the editing of zone information via the web; the DNS Secondary Service, through which IIJ handled secondary servers only; and the Domain Management Service for managing and maintaining domain registration.

Up to this point, JP domains were classified based on attributes such as co.jp (companies) and ac.jp (academic institutions). A domain is something that represents an organization, so you could only register one domain per organization. Then in 2001 came the release of a general-purpose JP domain system that did not tie domains to specific organizations or place limits on the number of domains registered. This prompted an increase in the number of domains being registered not

[*2] Burton G. Malkiel, Chapter 4, A Random Walk Down Wall Street.

just for individual organizations but also for specific products and brands. And so the number of domains registered and the use of the DNS Outsourcing Service / Secondary Service was growing every year.

It was no longer uncommon by this point for individuals with no organizational affiliation to also have their own domains. So in March 2002, we launched the IIJmio Personal Domain Service, making it possible for people to use email, web, and DNS hosting via their own domain at a low price although without all the bells and whistles, and then in March 2003, we launched the DNS hosting-only IIJmio Simple DNS Service.

The three services previously mentioned—DNS Outsourcing Service, DNS Secondary Service, Domain Management Service—all went on to become long-lived services running for over 20 years, with features and capacity additions being made along the way. Of particular significance here were DNSSEC support and the Site Failover Option, an optional add-on service.

DNS is one of the Internet's essential component technologies, but the protocol was first designed back in the 1980s, so it also has shortcomings that are the result of certain issues either not being envisioned or not being seen as a problem. One such shortcoming is that it is difficult to detect when response packets are forged as part of cache poisoning or man-in-the-middle attacks. These require a lengthy discussion, so I will skip the details, but it was DNSSEC[*3] that made it possible to sign DNS information so that response recipients can confirm the authenticity of the information by validating signatures.

DNSSEC support commenced on the DNS root servers in July 2010, and the JP zone was DNSSEC signed in December 2010. IIJ's Domain Management Service and DNS Outsourcing Service added DNSSEC support in January 2011. DNSSEC necessitates some complicated work not previously involved in DNS operations, including generating signature keys and signing zones. To make DNSSEC available without the hassle, we set this up so that it would be done automatically on the IIJ server side.

As information stored in the DNS system was static, any change to the response required a manual rewrite of the information. The Site Failover Option released for IIJ's DNS Outsourcing Service in March 2015 improved webserver availability by making it possible to monitor webservers externally, quickly remove any server encountering some sort of failure from the DNS response and switch to a standby server, and automatically return it to the DNS information once the webserver had recovered.

4.4 2010s: Wrestling with Attacks

■ The rise of DDoS attacks

The 2010s saw DDoS (distributed denial of service) attacks by botnets increase in scale, and we had to scramble to implement countermeasures.

DDoS attacks saturate server processing capacity by flooding the server with simultaneous requests from a large number of devices, resulting in a loss of availability. In the 2000s, computer viruses evolved rapidly into what are called worms, which, upon infecting a device, are able to spread themselves broadly to other systems, and they subsequently developed the ability to coordinate to form botnets. DDoS attacks in which the many bots comprising a botnet act at the behest of an attacker sending commands became a frequent occurrence all over the world.

Internet traffic, meanwhile, continued to grow rapidly, with the use of CDNs (content delivery networks) designed to efficiently deliver web content also spreading, and small, garden-variety DDoS attacks were no longer able to bring down services running on servers designed to handle huge amounts of traffic.

[*3] For example, see "What is DNSSEC?" (https://jprs.jp/dnssec/doc/dnssec.pdf, in Japanese).

Now, with DNS, only a few hundred bytes at most are exchanged at any one time, and because of the efficient caching mechanism too, the load on CPU, memory, and network bandwidth resources is miniscule relative to the loads imposed by web and email protocols and the like. So while the performance and bandwidth of webservers have continued to rise, it has long been the case that DNS servers are allocated only a minimum of resources.

In many cases, the attacker's goal is to render a website unavailable. The target of an attack need not be the webserver itself if this goal can be achieved by other means. To access a website, you first need to know the site's IP address, so the goal can be also achieved by interrupting the mechanism for obtaining that IP address—i.e., the authoritative DNS server. Rather than targeting webservers protected by CDNs and thus able to withstand the onslaught of large amounts of attack resources, it is more efficient for attackers to target authoritative DNS servers, which are easily saturated by modest loads.

The October 2016 DDoS attacks on Dyn (later acquired by Oracle) are a prominent example of this[*4]. Dyn was a truly major provider of authoritative DNS services, with prominent global web services such as Twitter and Spotify being hosted by Dyn. Dyn's servers were the subject of DDoS attacks emanating from hundreds of thousands of devices over a period of six hours, rendering them unable to return a response, which made many of the domains using Dyn unreachable.

In 2012, four years before the attacks on Dyn, IIJ also suffered a large-scale DDoS attack against an authoritative DNS server. The attack was targeted at the domain of a customer whose web and DNS systems were hosted by IIJ. The attackers initially attacked the webserver but subsequently realized that the server was performant enough that they would not be able to bring it down. So they refocused their sights on authoritative DNS. IIJ's authoritative DNS servers had what was an abundance of resources for the time, but this was utterly insufficient to withstand a DDoS attack designed to marshal enough resources to take down a broadband webserver, and thus the target server struggled to respond to requests.

This incident prompted a major shift in DNS server design philosophy at IIJ. The DNS server network configuration changed significantly from what it had been before. Multiple defenses were implemented, which included ensuring sufficient bandwidth to withstand saturation attacks, creating a mechanism for using anycast to localize the impact even if bandwidth was saturated, and isolating the DNS servers on a dedicated network so that the impact of attacks would not ripple into other services. The equipment configuration changes incorporating these measures were rolled out progressively on both the authoritative DNS servers used by the DNS Outsourcing Service and the like and the caching DNS servers used in our connectivity services.

■ Open resolver challenges

IIJ hasn't been exclusively on the receiving end of DDoS attacks. IIJ's DNS servers have, unfortunately, also been used as a springboard for DDoS attacks.

DNS primarily uses UDP as its lower-layer protocol, and UDP makes it easier for clients to spoof IP addresses than TCP. The DNS response packet size can also be tens to hundreds of times larger than for queries. A malicious attacker can take advantage of this by sending queries with the source IP address spoofed to be that of the target to a DNS server that will act as a stepping stone, such that it returns a response to that IP address with an amplified packet size, which can saturate the target network's bandwidth. Such attacks are called DNS amplification attacks (DNS amp) or DNS reflection attacks (Figure 1).

[*4] Wikipedia, "DDoS attacks on Dyn" (https://en.wikipedia.org/wiki/DDoS_attacks_on_Dyn).

DNS amp attacks work because DNS servers return a response to spoofed IP addresses, so these attacks could be prevented by not responding to queries from spoofed IP addresses. But because of the way UDP works, it is difficult to detect spoofing.

Caching DNS servers are usually set up for use by a single organization, so only making it available to users within that organization is generally fine. Not responding to external queries would mean that large responses are not sent outside of the organization, even if source IP addresses are spoofed, thus making it impossible to use the organization's server as a DNS amp stepping stone. Yet for a long time in the wake of the Internet's spirit-of-mutual-aid era, it remained uncommon to impose such restrictions on caching DNS servers. IIJ's caching DNS servers were no exception; they too were open resolvers with no access restrictions.

DDoS attacks were prevalent during this period, and malicious attackers began turning their gaze to these open resolvers and using them as stepping stones. We knew that restricting access would prevent our servers from being used as stepping stones, but doing so would also make them unavailable to users using IIJ's servers for their intended purpose and not nefarious ones. After struggling with this dilemma at length, in December 2013 we finally changed our settings to prevent access to IIJ's caching DNS servers from outside of the IIJ network.

Open resolver countermeasures did not end here. While we had dealt with IIJ's DNS servers, there were many cases in which caching DNS servers installed by users and the DNS functions of users' routers were acting as open resolvers and thus used as attack stepping stones, so we had to contact these users and ask them to take appropriate steps. Thanks not only to IIJ's efforts in this regard but also to diligent efforts around the world, the incidence of DDoS attacks leveraging DNS began to die down.

4.5 2020s: Further Developments

■ Encrypted DNS

DNS is public information. So initially, the emphasis was on the information not being tampered with (integrity) rather than on it not being eavesdropped (confidentiality). DNSSEC, released in 2010, is also a mechanism for ensuring integrity. But following the Snowden Incident[*5] in 2013, revealing that the US NSA was collecting large amounts of personal information, the Internet Engineering Task Force (IETF, a volunteer organization tasked with developing Internet standards) declared that "pervasive monitoring is an attack"[*6] and called for future Internet protocols to be equipped with mechanisms for mitigating widespread surveillance. The Snowden incident revealed

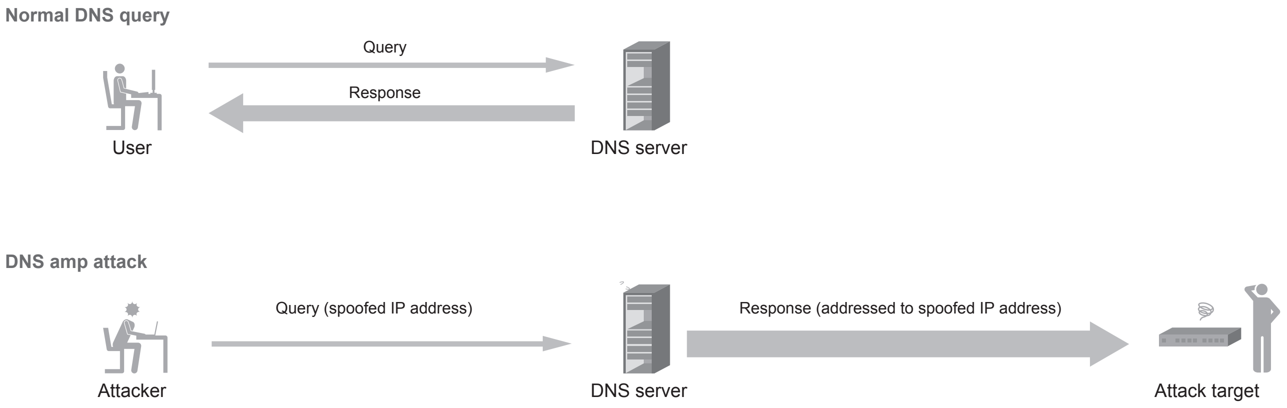

Figure 1: DNS amp

[*5] Wikipedia, "Edward Snowden" (https://en.wikipedia.org/wiki/Edward_Snowden).

[*6] RFC 7258: Pervasive Monitoring is an Attack.

that DNS was also a target of surveillance, and so it was concluded that, despite DNS being public, the information being sought was a matter of personal privacy and that confidentiality would be crucial to DNS going forward.

This led to the DNS over TLS (DoT) and DNS over HTTPS (DoH) standards. Traditional DNS puts DNS messages directly on top of UDP or TCP, but DoT and DoH put DNS messages on top of (respectively) TLS and HTTPS layers to prevent eavesdropping by third parties.

From 2018 to 2019, public DNS services such as Google Public DNS and Cloudflare 1.1.1.1 adopted DoT and DoH one after another, with client-side support via web browsers and OSs continuing to roll out.

Some issues still remain at present. DoT and DoH only encrypt communications between clients and caching DNS servers, not between caching DNS servers and authoritative DNS servers, and mechanisms for automating DoT/DoH servers are not yet widespread. That said, these protocols are expected to play an important role in the future.

This led to the May 2019 launch of the IIJ Public DNS Service, an experimental service for the purpose of verifying the technology. DoT and DoH do not use UDP and thus do not carry the risk of being used in DNS amp attacks, so we made servers running these protocols available as open resolvers to non-IIJ users. Support for DoT and DoH has since gradually been expanded to caching DNS services used in connectivity services.

■ New authoritative DNS service

Since the dawn of the Internet, people have been saying that multiple authoritative DNS servers should be set up to improve availability. Although the number of DDoS attacks using DNS as a stepping stone fell away, DDoS attacks themselves have actually been on the rise since. As such, an idea that is gaining traction in recent years, particularly for large sites, is that of distributing zones among multiple DNS operators so that name resolution can continue even if any particular operator experiences a fault that renders its servers unresponsive.

Although we had continued to enhance the features of the DNS Outsourcing Service and DNS Secondary Service launched in 2000, the focus was on the basic function of receiving and responding to queries. They did not have functionality for coordinating among multiple operators. For this reason, we set about overhauling the services, which also included bolstering other administrative functionality, and these efforts culminated in the release of the IIJ DNS Platform Service in November 2019. The service allows admins to freely configure their systems in ways that were not possible with the previous services. They can, for instance, use IIJ as the primary server and another operator as the secondary, or DNSSEC sign zones on the IIJ server transferred from the user’s primary server. We also launched the IIJ DNS Traffic Management Service in March 2022 as successor to the Site Failover Option.

4.6 Conclusion

We have taken a whirlwind tour back through IIJ’s 30-year history with a focus on DNS. Many other pertinent anecdotes could have filled these pages, but space limitations necessitated their omission.

The DNS protocol has been around since the old days, but is not stagnant and is constantly evolving. Now, as ever, it remains a cornerstone of the Internet’s foundations. Looking ahead, IIJ plans to continue actively incorporating advanced features while providing robust, flexible DNS services.

Takanori Yamaguchi

Application Service Department, Network Division, IIJ. Mr. Yamaguchi works on the development of DNS services and the like.