

IIJとDNSの30年

山口崇徳@IIJ

2023/06/23 DNS Summer Day 2023

IIJとDNSの30年

- 1992年12月 インターネットイニシアティブ企画設立
- 1993年5月 インターネットイニシアティブに社名変更
- 1993年11月 国内初の商用インターネット接続サービス開始

- それから今年で30年
- DNSの観点で振り返ります

DNSはなかった

1993年

- 1993年11月 「インターネット接続サービス」 開始
- 提供するものは、あくまで接続するところだけ
 - DNSをはじめ、メール、NetNewsなど、すべて利用者が用意
- 商用国内初とはいえ、学術ネットワークとしてのインターネットを知っている利用者ばかり
 - 必要なものは自分で用意するか、参加者の相互扶助でなんとかする、というのが当時の共通認識
 - ユーザ側もIIJが提供するとは思ってない

最初のDNSサーバ

1994年

- 1994年5月 「ダイアルアップIPサービス」 開始
 - 専用線ではなく、電話回線を利用して必要なときだけ接続するためのサービス
 - クライアントとしての利用が主で、サーバを構築・運用する用途にはそぐわない
 - キャッシュDNSサーバ(だけ)はIIJが用意することに
- 権威DNSサーバはユーザが運用する前提なのは変わらず
 - ただし、ビジネスとしてではなく相互扶助の一環として、一部のセカンダリは引き受けていた

JPセカンダリ

1994年～

- 相互扶助の一環で引き受けていたセカンダリゾーン
 - 3系列DNSのうちの海外向け系列とマージ系列
 - 3系列DNS何それ?という話は森下さんがtweetしてくれると思います:-)
- IJに依頼されることになった経緯がわかる文書は現在もJPNIC上で閲覧可能
 - 第8回～第10回JPNIC運営委員会のDNS管理グループ作業報告
 - <https://www.nic.ad.jp/ja/materials/committee/oldindex.html>
 - <https://www.nic.ad.jp/ja/materials/committee/1994/0510/shiryou-2-4-1.html>
- 以後、現在に至るまでJPセカンダリの運用が続いている

インターネットの普及

1990年代中盤

- ・1994年9月 INTERNET magazine創刊(インプレス)
- ・1995年11月 Windows95 国内発売
- ・この時期に前後して多数のISPが誕生
- ・1996年12月 「IJJ4U」開始
 - ・ 大規模な個人向け接続サービス
 - ・ 「2台のキャッシュDNSサーバを異なるネットワークセグメントに設置」という今とっては常識の構成を初めて採用してユーザに提供

インターネットの普及

1990年代中盤

- 1997年11月 「IJエコノミー」 開始
 - SOHO向け廉価版専用線サービス
 - 法人向け接続サービスでキャッシュDNSサーバが標準提供になった最初のサービス
- キャッシュDNSサービスの基礎が固まる
 - その後、ADSLやら光やら接続サービスの形態は時代とともに変遷するも、キャッシュDNSの基本は変わっていない

ドットコムバブル

1999~2001年

- 1999年 インターネット関連銘柄を中心に米国株式が高騰
 - インターネットとは無関係な企業でも、「なんとかドットコム」という社名に変更するだけで値上がり
- 2001年 バブル崩壊
 - いまでは「ドットコムバブル」や「インターネットバブル」として知られる
- 株価は一時的なバブルだったが、企業が「ドットコム」なドメイン名を持つ習慣は完全に定着

権威DNSサービスの開始

2000年～

- ドメイン名を取得しても、DNSがなければ使えない
- インターネット黎明期は過ぎ、自分でDNSサーバを構築・運用するノウハウを持たない人が大半に
- 2000年3月、初のDNS単独サービスを開始
 - 「DNSアウトソースサービス」：プライマリとセカンダリ、Webでのゾーン編集
 - 「DNSセカンダリサービス」：セカンダリのみ
 - 「ドメイン管理サービス」：ドメイン名の登録、維持管理
- 20年以上継続する長寿サービスに

汎用JPドメイン

2001年～

- ドメイン名とは組織を表すものだった
 - co.jp(企業)、ac.jp(学術機関)など、組織属性による分類
 - comやnetなどのgTLDも元々は組織属性を表していた
- 2001年 汎用JPドメイン
 - 組織属性に紐づかないドメイン名へ(example.jp)
 - 1組織1ドメイン名の制限がなくなる
- 組織ではなく、商品やブランドごとにドメインを持つことも一般的に
- ドメイン登録数、DNSアウトソースサービス/セカンダリサービスの利用拡大

個人でのドメイン利用

2002年～

- ・「ドメインは組織を表すもの」ではなくなったことで、組織に属さない個人によるドメイン取得も増える
- ・2002年3月 「IJmioパーソナルドメインサービス」
 - ・ 独自ドメインによるWeb+メール+権威DNSのセット
- ・2003年3月 「IJmioシンプルDNSサービス」
 - ・ 権威DNSホスティングのみ

DNSアウトソースサービスの機能追加

- 随時機能拡張を重ねてきたけど、とくに大きなものは以下
- 2011年1月 DNSSEC対応
 - 元々のDNSは中間者攻撃などで応答を改竄されても検知が困難
 - DNSの登録情報に電子署名を付与し、それを検証することで完全性を保証する仕組み
- 2015年3月 「サイトフェイルオーバーオプション」
 - Webサーバ(など)を監視し、その結果に応じて動的にDNSサーバの応答を変化させるオプションサービス
 - Webの可用性向上

DDoS攻撃との戦い

2000年代後半～

- コンピュータウィルス → ワーム → botnet
- 2000年代後半からbotnetによるDDoS攻撃が活発化
- CDN (content delivery network)の普及
 - 大規模コンテンツ配信に特化したWebサーバ
 - 潤沢なリソースにより、ある程度のDDoS攻撃には耐えられる
- が、DNSは……
 - ネットワーク帯域やCPU等をほとんど必要としない
 - 最低限のリソースがあれば十分に運用できる

DDoS攻撃との戦い

2000年代後半～

- 攻撃者の目的はWeb閲覧不能
 - 攻撃対象がWebである必要はない
 - WebサーバのIPアドレスを知るために仕組み = DNSを攻撃しても同じ効果
- CDNに守られたWebサービスより、リソースの貧弱なDNSサーバの方が簡単に落とせる
- 2012年 IIJにDDoS攻撃
- 2016年 DynにDDoS攻撃 → 世界的に大きな影響

DDoS攻撃対策

2012年～

- 2012年に攻撃を受けて以降、設計思想を大きく転換
 - DNSサーバを攻撃されても耐えられるよう十分なリソースを確保する
 - Anycastにより被害を局所化できるようにする
 - Anycast: 同一のIPアドレスを地理的に異なる拠点で利用する仕組み
 - 特定地域を担当する拠点に攻撃が集中しても、それ以外の地域には影響がない
 - DNS以外のIJサービスに被害が波及しないよう、専用ネットワークへの分離
- サービス仕様は変わらないが、内部的に大きな構成変更
 - 権威、キャッシュとも、数年かけて移行

オープンリゾルバ問題

2010年代

- DNS amplification attack
 - 「もしもしヤマグチですけど寿司を10人前出前して」という注文を偽物のヤマグチがすると、本物のヤマグチさんに寿司が届く
 - …というのをDNSでやるような攻撃
 - 2010年代、DDoS攻撃の手法として盛んに使われた
- アクセス制限のないキャッシュDNSサーバ(オープンリゾルバ)はDNS ampの踏み台にされやすい
 - が、インターネットに相互扶助の精神が強かった時代から、キャッシュDNSサーバはアクセス制限をかけないことが多かった

オープンリゾルバ対策

2013年～

- キャッシュDNSサーバにアクセス制限すると
 - DNS ampの踏み台として使うことはできなくなる
 - IJ網外から本来の用途でDNSを利用していたユーザも使えなくなってしまう
- 2013年12月 アクセス制限実施
 - その後も、お客様設備がオープンリゾルバになっている事例を見つけて対処を要請する活動が続く
- しだいにDNS ampは鎮静化
 - なくなっていないし、DNS ampを使わないDDoS攻撃はますます増える一方…

暗号化DNS

2010年代～

- 2013年 スノーデン事件
 - 米政府組織による大規模インターネット盗聴
 - 盗聴に耐える仕組みが求められる
- DNS over HTTPS/TLS
 - DNSを暗号化する仕組み
 - 2016～2018 プロトコル仕様の策定
 - 2017～ パブリックDNSサービスや各種ブラウザでの実装

IIJと暗号化DNS

2019年～

- 2019年5月 「IIJ Public DNSサービス」
 - DNS over HTTPS/TLS(だけ)に対応したキャッシュDNSサーバ
 - IIJユーザ以外も利用可能な実験サービス
- 2020年1月 各接続サービスで提供しているキャッシュDNSサーバでDoH/DoTに対応
- 暗号化DNSはまだ発展途上
 - 暗号化DNSを自動設定する仕組みが普及していない
 - 権威DNSの暗号化仕様がでない

新しい権威DNSサービス

2019年～

- 2000年に開始されたDNSアウトソースサービス/セカンダリサービスは機能の拡張、設備増強を繰り返してきたが、建て増しはそろそろ限界
- 2019年11月 「IIJ DNSプラットフォームサービス」
 - IIJをプライマリ、他社サービスをセカンダリに利用
 - プライマリから転送されたゾーンをIIJセカンダリでDNSSEC署名
 - ……など、これまでできなかった様々な利用形態にも対応
- 2022年3月 「IIJ DNSトラフィックマネージメントサービス」
 - サイトフェイルオーバーオプションの後継

新しいキャッシュDNSサービス

2023年～

- これまでのキャッシュDNSサーバは、接続サービスの契約者向け
- 2023年6月 「IIJ xSPプラットフォームサービス/キャッシュDNS」 開始
 - 接続サービスに紐づかない、初のキャッシュDNS単独のサービス
 - ISP、DC事業者向けのキャッシュDNSサーバのアウトソース

まとめ

- 30年いろんなことがありました
 - DNSはインターネットを支える根幹技術のひとつ
 - 古いままではなく、今も進化を続けている
 - これからも進化を取り入れつつ安定サービスを提供
-
- 今回の話はIIJの発行する季刊技術レポート IIR vol.59にも掲載されています
 - <https://www.ij.ad.jp/dev/report/iir/>