

まちで見かけた変なIPv6

<公開版>

株式会社ビーコンエヌシー
データセンター事業部
國武 功一

あわてるな！

これは孔明の罠だ！



IPv6に対応したいけど接続性ない

Many Thanks to
Tokyo6to4!

- 移行技術に6to4なる技術があるらしい
 - 手元のサーバにはIPv4グローバルアドレスが

www.example.co.jp. AAAA 2002:c000:201::80

を登録してしまった事例

IPv6に対応したいけど接続性ない

- IPv4互換アドレスというものがあるらしい

www.example.co.jp. AAAA ::192.0.2.1

を登録してしまった事例

IPv6に対応したいけど接続性ない

- IPv4射影アドレスというものがあるらしい

www.example.co.jp. AAAA ::ffff:192.0.2.1

みなまで言う必要ないですね？

正確な知識を得ていないがためのミス

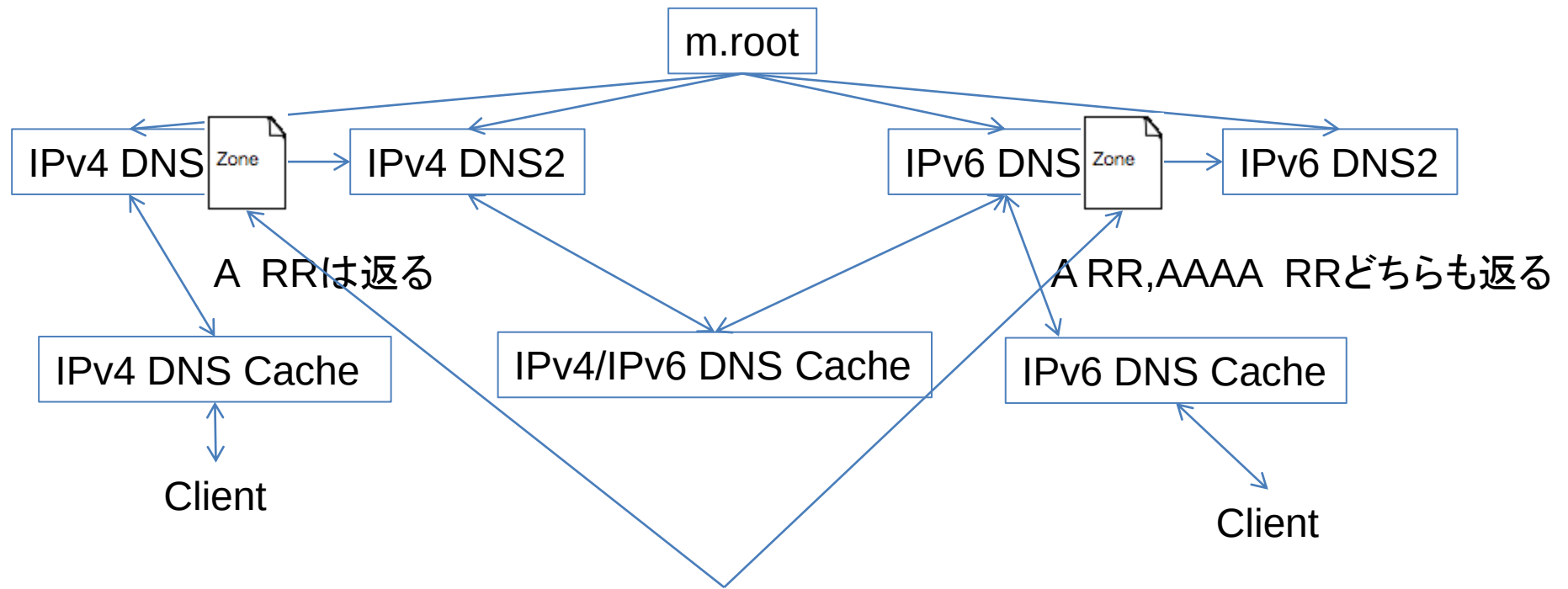
- 6to4 のアドレスはトンネルプロトコルであるため、誤りではないが、多くのクライアントでは、優先度が低く、実質的に利用されない。
- IPv4互換アドレス・IPv4射影アドレスは、クライアント、サーバにおける取扱上の問題であり、実際にIPv6パケットが送られるわけではない。

混ぜるな危険①!

だけど分けすぎも...

DNS権威サーバをIPv4/IPv6で分けました！

- 既存環境に影響を与えないために、完全に分離します！（もしくはさせらましadlalkjsdklf



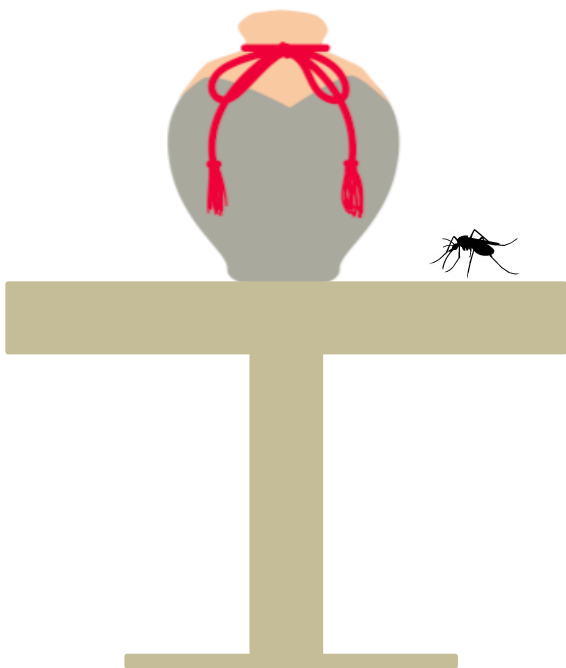
混ぜちゃだめなんだから、別々にゾーン情報は管理！

DNSサーバをIPv4/IPv6で分けました！

- これってなにが起きる、起き得るの？
 - IPv4とIPv6のDNSサーバ間でシリアル番号が異なる...
 - » 片方が障害起きた/復旧したときに.....
 - そもそもクライアントがIPv4/IPv6のどちらかが話せるかどうかは関係ない...

久しぶりに見たら、シリアル一緒になってた！
運用改善！.....苦労が偲ばれます

攻撃者に情報を与えるな！



攻撃者に情報を与えるな！

- 未知のパケットが来たら、攻撃の可能性がある。
Rejectではなく、Drop(Silent Discard)が望ましい！

という実装方針だった？

某GSLBに実装されたであろうDNSサーバは、SOA, NS, とか、A以外はREFUSE返すのに、AAAAだけ Timeoutしてくれる

Happy Eyeballs 最高？！

と思ってたんですが

dig @権威サーバ <問題のFQDN> <RR Type>

のように、

A6, AAAA, AFSDB, APL, CERT, CNAME, DHCID, DLV, DNAME, DNSKEY, DS, HIP, IPSECKEY, KEY, KX, LOC, MX, NAPTR, NS, NSEC, NSEC3, NSEC3PARAM, PTR, RRSIG, RP, SIG, SOA, SPF, SRV, SSHFP, TA, TKEY, TLSA, TSIG, TXT, MD, MF, MAILA, MB, MG, MR, MINFO, MAILB, NULL, UNSPEC

などなど試しましたが、Timeoutは A6, AAAAだけでした...比較的最近のRFC6698で定義されているTLSAも REFUSEで返していることから、意識的にIPv6関連だけタイムアウトする実装？

私も町で見かけたい！



こんなところから

- AAAA対応リストから、::ffff とかで検索してみるとか
- 某省庁のサイトを注意深く観察
 - あらゆるサンプルの宝庫。むしろトラブルシューティングの見本として保全すべき



これから見かける光景？

- リプレイスの時になんで言わなかったんだ！
 - PHP4->PHP5の話再び？
 - PHP4もうサポートされないじゃない、なんで前回の改修の時にRHEL5に上げましょうって提案しなかったの？
 - IPv6の時にも？
 - » IPv4アドレスの枯渇が叫ばれてることがわかってて、なんで前回のシステム更新の時にIPv6対応について、言わなかったんだ！



って言われちゃうんですかね？

なにはともあれ

- 笑っていられるうちに、IPv6の変なところ共有しましょう
- 直せるものなら、直しておきましょう！
- というフェーズは終わりつつある？どうなんでしょうか...教えてください！ 懇親会とかで 

