DNSなんでも相談室2021(夏)

怒りのGTM編

2021年6月25日

株式会社インターネットイニシアティブ
ネットワーク本部アプリケーション開発部DNS技術課
其田　学

DNSなんでも相談室では、
IIJ社内のDNSに関する問い合わせ、相談を受けています
その中でも、今回はフルリゾルバ関連のものを紹介します

注意事項

本発表内のドメイン名は、実際のドメイン名とはなんの関係もありません
また、組織、団体名も実際の組織、団体名とはなんの関係もありません

この後出てくる設定イメージや、動作は、外部から確認した挙動を元に
作成しています。実際の設定とは異なる場合があります。

TL;DR

GTM (現BIG-IP DNS)は、正しく設定して用法を守りましょう。。

問い合わせ内容
「御社のキャッシュDNSサーバが、うちのドメイン名の名前解決できないんだけど、なんとかしろ」

運用T
「ふむふむ、とりあえずdig すっか」

```
$ dig trader.XXXX.com.
trader.XXXX.com.        300        IN        CNAME        trader.gslb.XXXX.com.
```

運用T
「gslb ….　あっ察し 」

ゾーンとして、応答がちゃんとできていない
- Aは答えるけど、他のRRTYPEはDROPしてたり

```
$ dig  trader.gslb.XXXX.com. A
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34882
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
trader.gslb.XXXX.com.    30        IN        A         X.X.X.X
```

```
$ dig  trader.gslb.XXXX.com. AAAA
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18056
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;trader.gslb.XXXX.com.              IN        AAAA
```

```
$ dig  trader.gslb.XXXX.com.  SOA
(応答がない)
```

「きっとこのタイミングだけ、疎通がなかったに違いない」

ゾーンとして、応答がちゃんとできていない

- Aは答えるけど、他のRRTYPEはREFUSED

```
$ dig  trader.gslb.YYYY.com. A
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34882
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
trader.gslb.YYYY.com.     30        IN        A         X.X.X.X
```

```
$ dig  trader.gslb.YYYY.com. AAAA
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 47053
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
```

「このNAME+TYPEだけRefusedなのか。そんなことある？」

ゾーンとして、応答がちゃんとできていない

- Aは答えるけど、他のRRTYPEはNXDOMAIN！

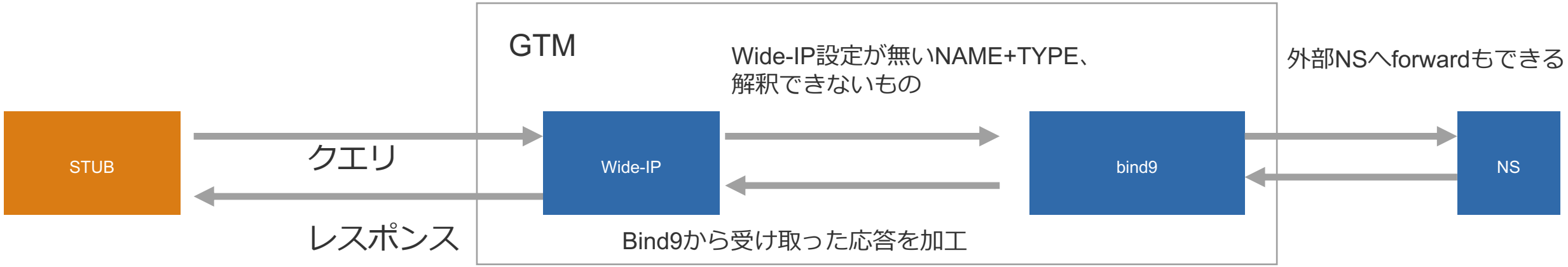
```
$ dig  trader.gslb.ZZZZ.com. A
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34882
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; ANSWER SECTION:
trader.gslb.WWWW.com. 30        IN        A         X.X.X.X
```

```
$ dig  trader.gslb.ZZZZ.com. AAAA
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 47053
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
```

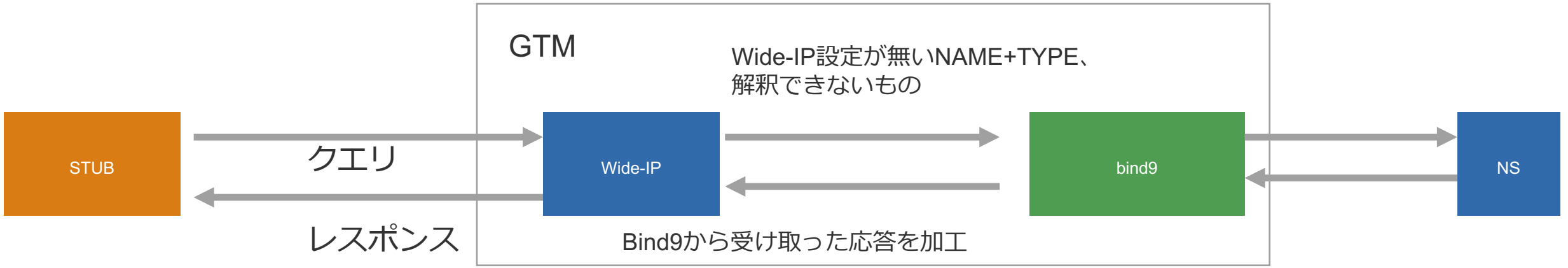
「AはNOERRORなので、名前はある、なのに、NXDOMAIN、矛盾するもう完全にアウト」

（きちんと触ったことがないのでイメージです）



リクエストは、一旦Wide-IPで受けて、ロードバランス設定が
有るNAME+TYPEは、この機能でレスポンスを返している
それ以外のクエリや、解釈できないクエリは、backendのBind9または
forward先のNSがリクエストを返す

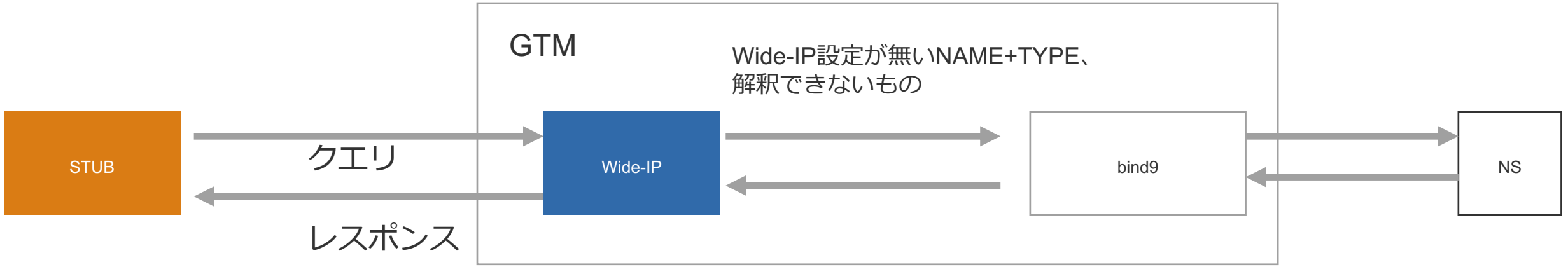
（きちんと触ったことがないのでイメージです）



Bind9またはforward先のNSにゾーンが設定されていても、
対応する名前のレコードがない場合、**NXDOMAIN**が返る。
また、レコードがあったとしても、**古いA,AAAAレコード**の場合もある。

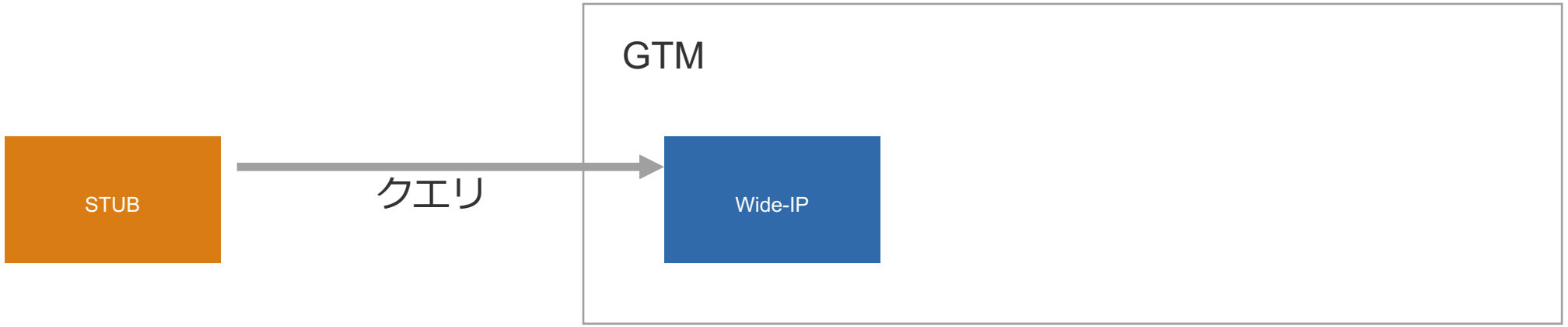
以前 DNS COOKIEが解釈できなくて、bind9に落ちたが、
bind9のレコードが古くアクセスできない事例があった

（きちんと触ったことがないのでイメージです）



Bind9またはforward先のNSにゾーンに、このクエリに対応するゾーンが無い場合、
突き抜けてきたクエリーに対応するゾーンが無いので**Refused**を返す

（きちんと触ったことがないのでイメージです）



bind9設定が無い場合は、応答を返しません。**DROP**されます

何が問題か？

- **問題しかない**
- NXDOMAIN -> MIN TTL間は名前が引かれない
- DROP、SERVFAIL ->サーバ異常と認識される。
  - 次回の名前解決で使用されないこともある
- QNAME Minimizationが有効なフルリゾルバでは、ゾーンのNSが引ける必要がある
  - 今時のUnboundでは引けないと思った方がいい

（きちんと触ったことがないのでイメージです）

Wide-IP部分で、A,AAAAの設定をした場合、
標準だと、Wide-IPに追加すると、Bind9の設定も入る
内蔵のBind9ではなく外部のNSを使う場合、外部NSに以下の作業が必要

1. Bind9の設定で、移譲された名前のゾーンを作成
2. A,AAAAの設定同名のレコードを作成する
3. RDATA部分はラストリゾート的なサーバを入れる

「そもそも内蔵のBIND9を使うのが望ましいって書いてあるんだが」

運用T
「（意訳)御社の権威DNSサーバの設定がおかしいですので、確認してください」

問い合わせ先
「。。。。。。」

理解してもらえることは、少数。
またGTMが入っているのは、クリティカルなシステムの場合が多く、
なかなか設定変更してもらえない。

BIND9自体が脆弱性という面で、機能をOFFにしている場合も多い

このパターンの問い合わせ2~3ヶ月に１回ぐらいは発生し、
最終的には解決できないパターンが多いです

まとめ

GTM (現BIG-IP DNS)は、正しく設定して用法を守りましょう。。

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ

IIJはいつもはじまりであり、未来です。