外部の権威DNSサービスに切り替える時にやらかした話

Internet Week 2024

株式会社ミライコミュニケーションネットワーク
田中温子

今日のお話

- 権威DNSサーバの自前運用に限界を感じ、外部の権威DNSサービスに出すことになったミライネット
- 移行するときに、NSの切り替えに失敗してやらかしたお話

自己紹介

名前：　田中温子

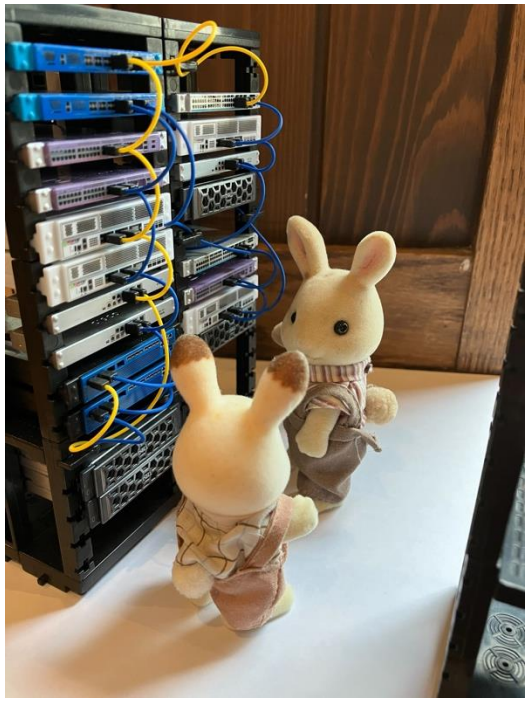
所属：　ミライコミュニケーションネットワーク
　　技術部運用チーム

仕事：　サーバーエンジニア

- ホスティングサーバの設計構築、障害対応
- メールサーバのリプレースをよくやっている

活動：　ChuNOGコアメンバー、DNSOPS.jp

マイブーム：　重ね煮



最初に結論を言います…

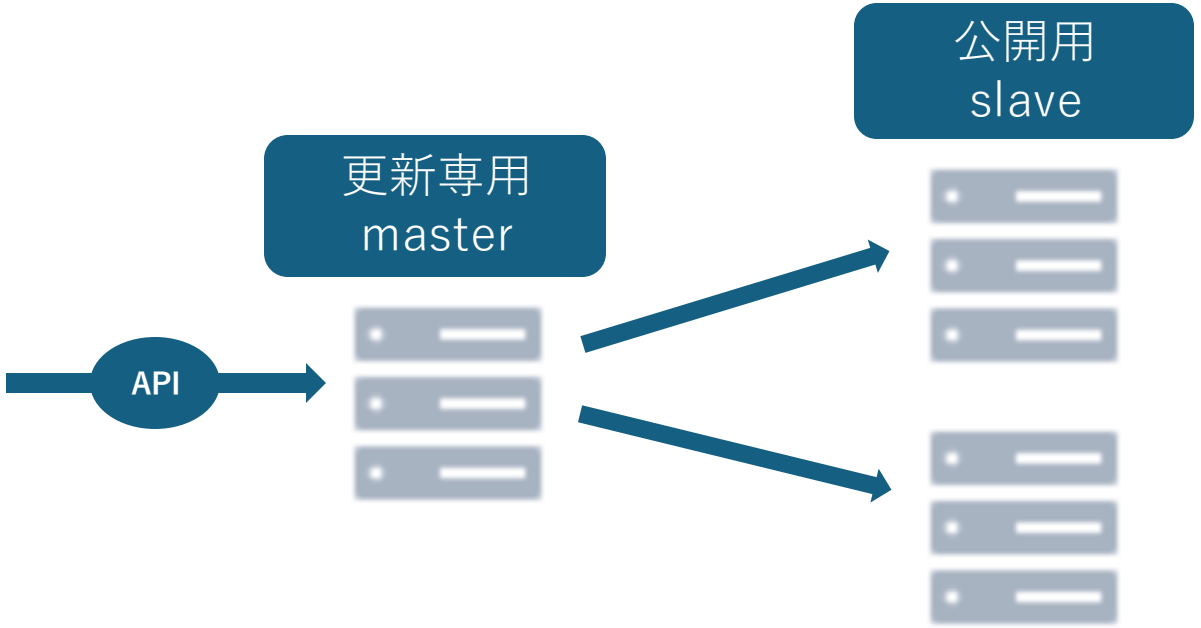
- **NSを変更する時に、CNAMEレコードを設定してはいけません**

※RFC1912抜粋

> **Having NS records pointing to a CNAME is bad** and may conflict badly with current BIND servers. In fact, current BIND implementations will ignore such records, possibly leading to a lame delegation.
> There is a certain amount of security checking done in BIND to prevent spoofing DNS NS records. Also, older BIND servers reportedly will get caught in an infinite query loop trying to figure out the address for the aliased nameserver, causing a continuous stream of DNS requests to be sent.

既存の権威DNSサーバの構成

- OSSで構築した権威DNSサーバが複数セット存在
- レコード編集ができる自社開発の管理画面を顧客へ提供
- ドメイン数は約2500



自社運用していた権威DNSサーバを、F5さんのDistributed Cloud DNSに出すことに

権威DNSサーバを切り替える流れ

（１）ゾーン情報を複製する

（２）Whois情報のNSを変更する

例

[ネームサーバ]	ns1.f5clouddns.com
[ネームサーバ]	ns2.f5clouddns.com

CNAMEで設定できるか検証してみた

- CNAMEレコードを新規作成

```
ns1.mirainet.co.jp.   IN  CNAME  ns1.f5clouddns.com.
ns2.mirainet.co.jp.   IN  CNAME  ns2.f5clouddns.com.
```

- 検証用のドメインのNSを変更

```
[ネームサーバ]          ns1.mirainet.co.jp
[ネームサーバ]          ns2.mirainet.co.jp
```

- 自社のキャッシュDNS、各種PublicDNS、キャリアから引けることを確認

この時、RFCを確認しなかった・・・

実際に自社のドメインを切り替えた

- 自社のドメインのNSを、CNAMEで設定して切り替えた

[ドメイン名]	MIRAI.XX.JP
[ネームサーバ]	ns1.mirainet.co.jp
[ネームサーバ]	ns2.mirainet.co.jp

- 自社のキャッシュDNS、各種PublicDNS、キャリアから引けることを確認

問題なく切り替えができた！と思っていたが・・・

何かが起き始める

- mirai.xx.jpのNSを切り替えてから2時間後、問い合わせが入る

A市、B市の複数ISP契約ユーザから、a-shi.example、
b-shi.exampleのWebサイトにアクセスできないそうです

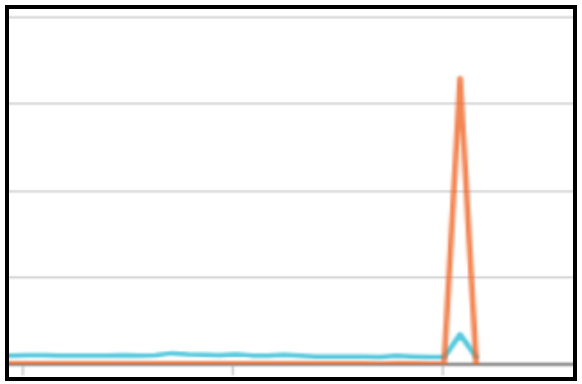
- a-shi.example、b-shi.exampleどちらもNSは、ns1.mirai.xx.jp/ns2.mirai.xx.jpを向いている

[ドメイン名]	a-shi.example
[ネームサーバ]	ns1.mirai.xx.jp
[ネームサーバ]	ns2.mirai.xx.jp

- ミライネットや、PublicDNS、キャリアからは問題なく引けることを確認

すぐには原因がわからなかった

- 該当時間、 ns1.mirai.xx.jp/ns2.mirai.xx.jpに多数のクエリが来ており、最初はそのせいにしてしまう



- だがクエリが減っても、A市、B市のISP契約ユーザからは引けない状態が継続

mirai.xx.jpのNS切り替えが影響していることにすぐには気づけなかった…

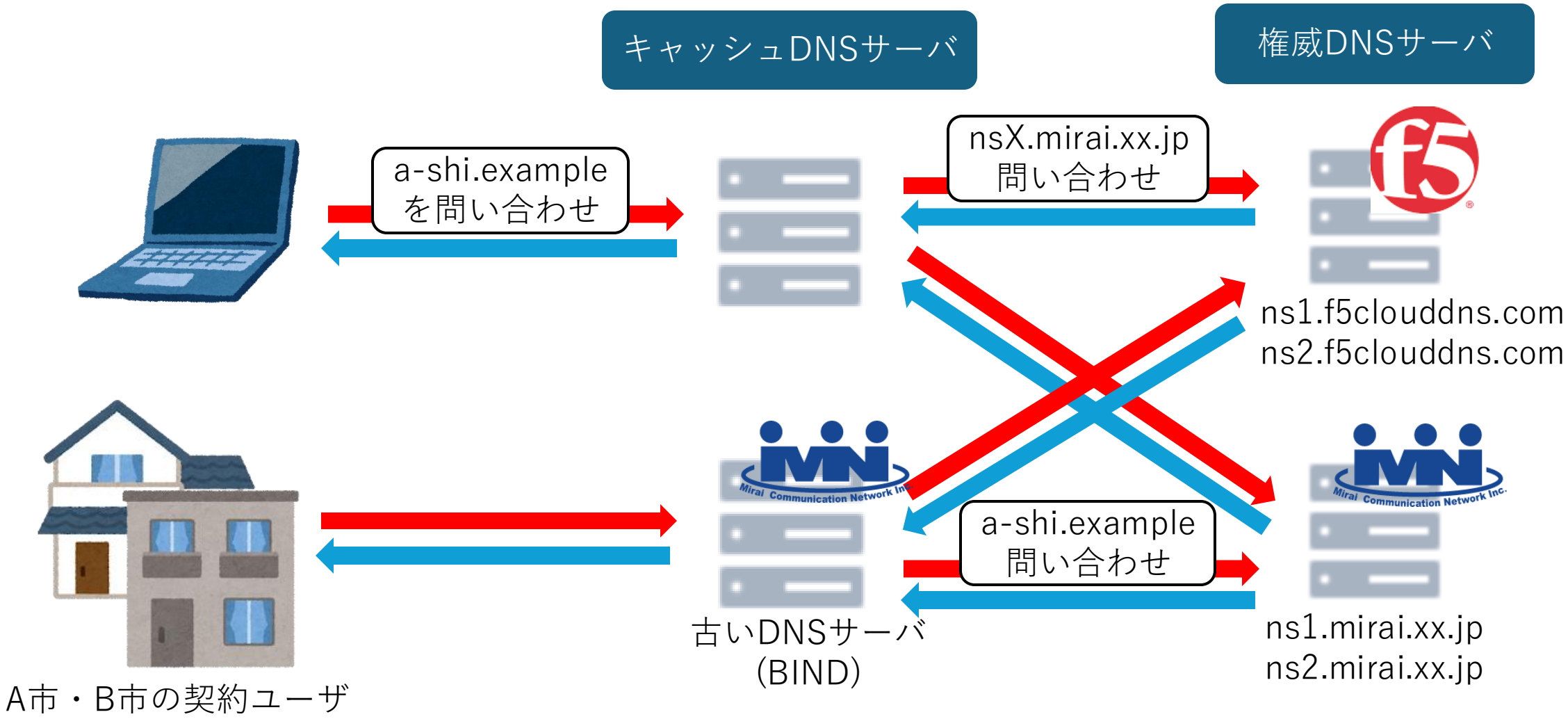
原因が判明する

- A市、B市のISP契約ユーザには、古いキャッシュDNSサーバのIPアドレスをDHCPで配布していた
- 古いキャッシュDNSサーバのログを確認すると、以下が出力

May 12 12:20:03 ns1 named[15315]: **skipping nameserver 'ns1.mirainet.co.jp' because it is a CNAME**, while resolving 'ns1.mirai.xx.jp/A'
May 12 12:20:03 ns1 named[15315]: skipping nameserver 'ns2.mirainet.co.jp' because it is a CNAME, while resolving 'ns2.mirai.xx.jp/A'

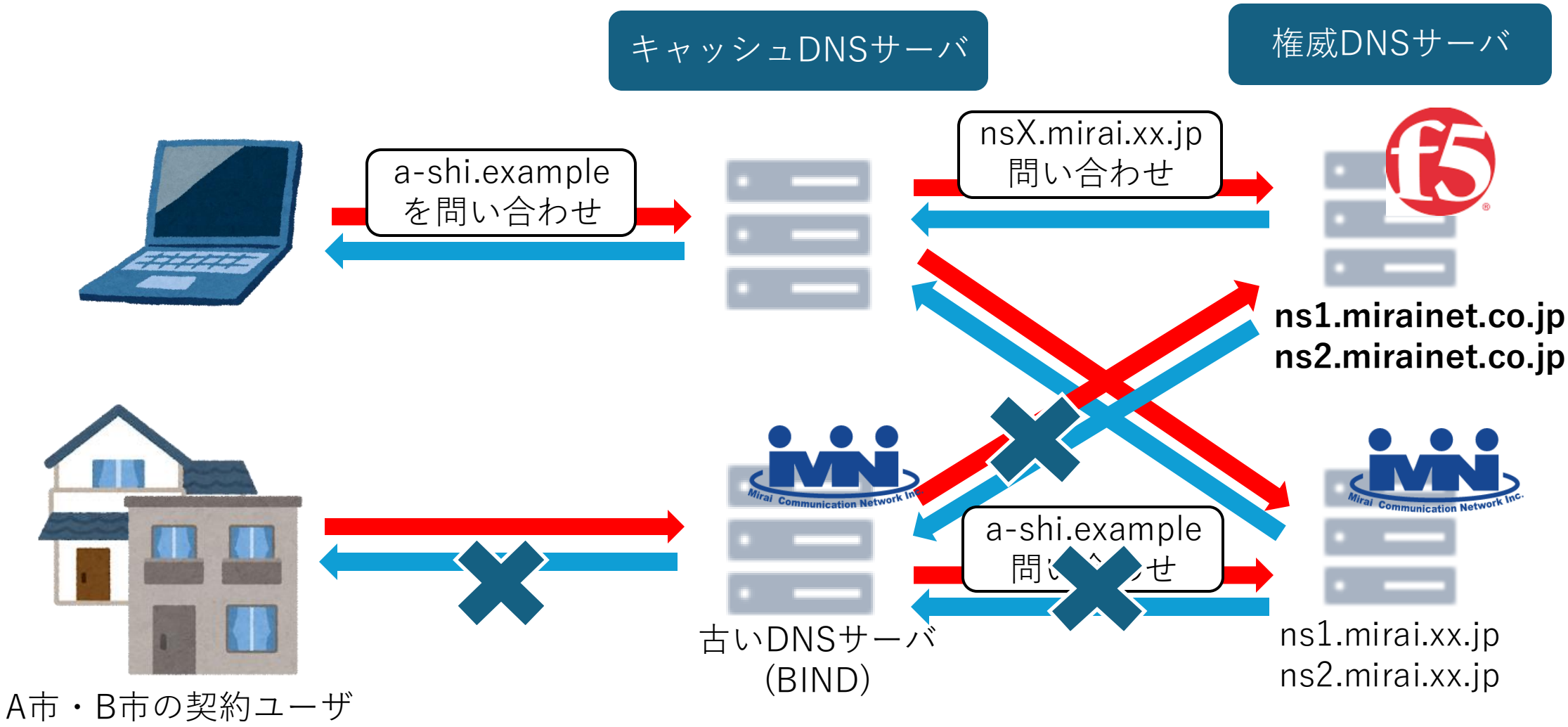
CNAMEで設定されているために、ネームサーバがスキップされて
該当ドメインのネームサーバの名前解決に失敗していた

何が起きていたか（正常な時）



※厳密にはルートサーバから問い合わせが発生しますが省略しています

何が起きていたか（NSがCNAMEの時）



キャッシュDNSサーバ(BIND)ではCNAMEのNSがskipされ名前解決に失敗していた

まとめ

- （再） NSはCNAMEで設定しないようにしましょう。知らないどこかのBINDのキャッシュDNSサーバでは、引けなくなってしまうかもしれません。
- （当たり前のことですが…）こんなことできるかな？って思ったら、実際にやってみるのはもちろん、RFCや、公式のドキュメントを確認しましょう


MN
Mirai Communication Network Inc.