DNSリゾルバの運用コスト削減への道

ヤフー株式会社 針山 拓海

自己紹介

- 針山 拓海(はりやま たくみ)
- 2016年 Yahoo! JAPANに新卒入社後、現在まで

  商用向けデータセンタネットワークの運用構築に従事
- 現在DNSリゾルバの運用・管理の主担当
- 長崎県長崎市出身

皆様にお伺いします

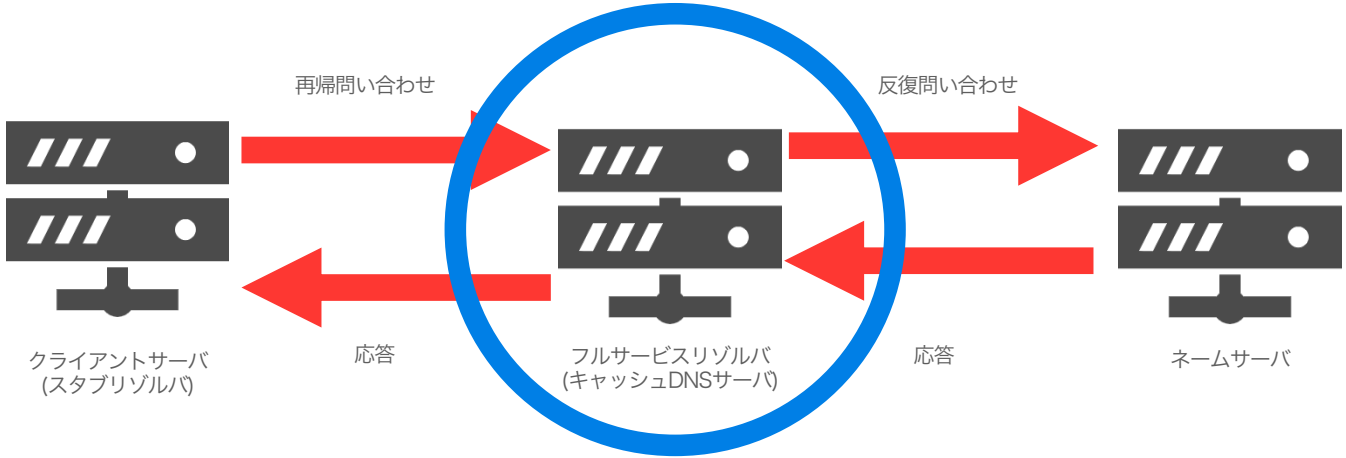
DNSリゾルバの運用って、大変ですよね？

今日のテーマ

- DNSリゾルバの運用コストを下げるために
  ヤフーDNSチームで取り組んだ内容のご紹介
- どうすればDNSリゾルバの運用コストを
  下げられるかの議論

(補足)今回のセッションでお話するヤフーのDNSリゾルバ

- データセンタ内サーバ向けのフルサービスリゾルバが対象



ヤフーのDNSリゾルバの利用用途

- データセンタ内サーバ向けのフルサービスリゾルバ
  - 社内環境間の通信のための名前解決など
  - メールサービスなど、外部疎通を行うサーバからは社外ドメインの名前解決リクエストも来る

画像：アフロ

DNSリゾルバの運用とは何をやっているのか

- 負加増に伴うサーバの増強
- 脆弱性対応
- 社内要望に伴うコンフィグの変更
- 障害対応

などなど

(過去の)ヤフーのDNSリゾルバの姿

- 拠点や用途ごとにVIPを建て、物理サーバをVIPメンバに収容する構成
  - ロードバランサを使用、L2DSR/L3DSR/L4 Inline構成
  - アプリケーションはBIND9系
- ヤフーのデータセンタに居るクライアントサーバはすべて
  自分と同じ拠点にいるDNSリゾルバを参照する
  - 2クラスタを参照することで冗長性の担保
  - どのリゾルバを参照するのかはDNSチーム側で管理

画像：アフロ

```
-bash-4.2$ cat /etc/resolv.conf
nameserver      XXX.XXX.XXX.XXX
nameserver      YYY.YYY.YYY.YYY
-bash-4.2$
```

(過去の)ヤフーのDNSリゾルバの問題点(1/3)

単純に台数が多く管理し辛い

- 特殊環境向けリゾルバが点在
- 多かった時期で300台近いサーバを管理
- クライアントは17万台強(2020年時点、含VM)
  - https://techblog.yahoo.co.jp/entry/2020102130034499/

画像：アフロ

サーバの台数が多いことによる運用コスト(1/2)

ファシリティ起因のサービスイン・アウト作業の頻発

- 上位NWや電源障害や、ラック最適利用のためのサーバ移設
- 影響を抑えるために一時的にサーバをVIPから隔離する作業が発生

設定変更やバージョンアップに時間がかかる

- BINDの脆弱性対応コストが非常に高い

サーバの台数が多いことによる運用コスト(2/2)

ラック冗長化とラック最適利用のバランスのジレンマ

- 耐障害性を考えるとリゾルバを収容するラックは分散させたい
- データセンタの運用コストを考えるとラックは集約させたい

サーバ台数が増えることによる故障発生確率の増加

- ものが増えるとその分なにか壊れる可能性は上がる

(過去の)ヤフーのDNSリゾルバの問題点(2/3)

物理サーバのスペックが低い

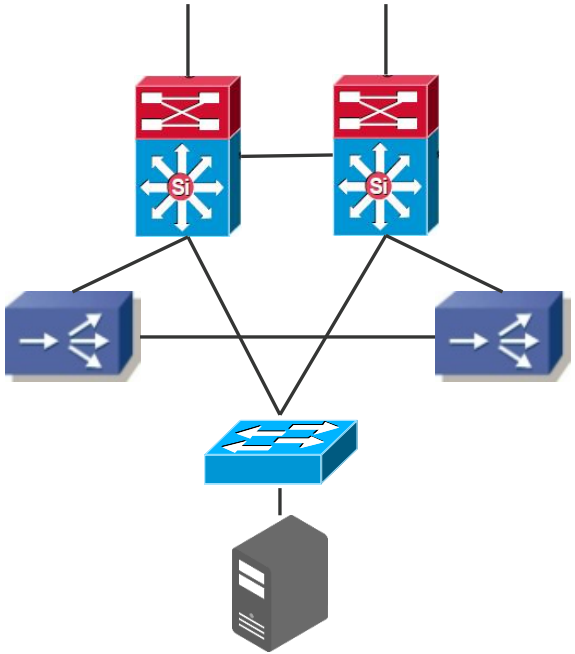
- 当時時点でも既に古めのサーバを使っていた
- 1台1台のスペックではなく数で性能を賄う方針

環境ごとにVIPのネットワーク構成が違う

- DSR(Direct Server Return)のVIP構成を中心に構築
- 物理サーバのNICスペックが低かった頃、
  2NIC利用によるスループット向上を期待してインライン構成のVIPを一部で導入

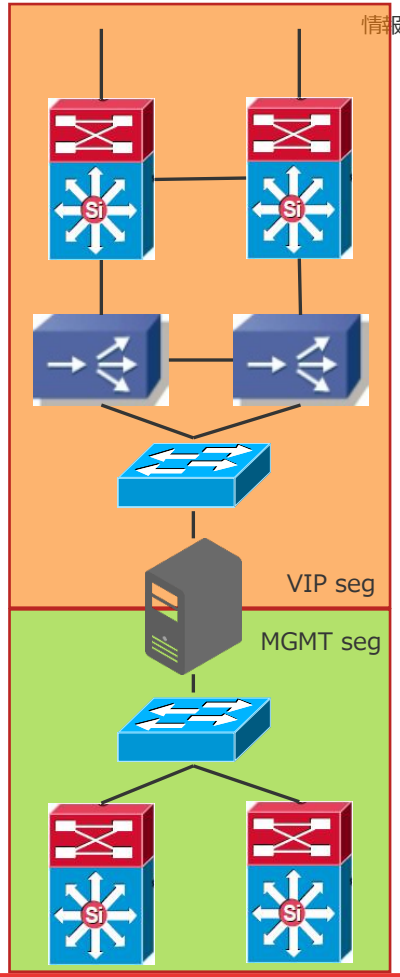
ヤフーでのDSR VIP構成例

- Y!ではHWLB VIPではDSR構成を取るのが主流
- Y!VIPでは殆どの通信が
  リクエストサイズ<<レスポンスサイズ
  レスポンスがLBを経由しないDSRはコスト的に有利
- 社内知見もDSR構成のほうが多い



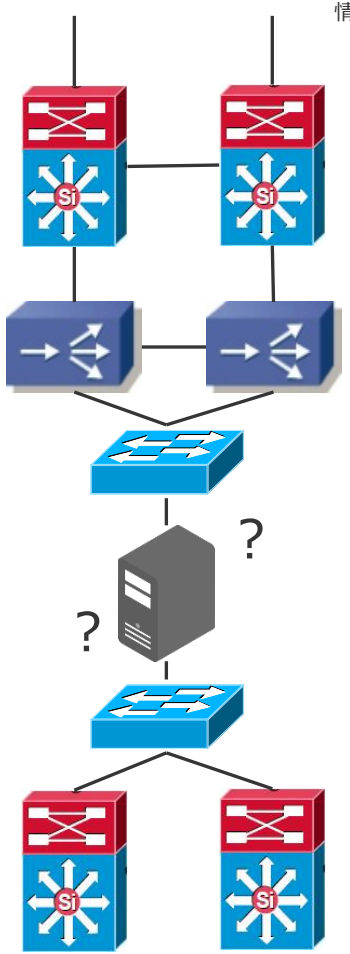
過去のインライン構成リゾルバVIP構成

- LB~サーバ通信とそれ以外の通信で
  サーバが使うNICを出し分ける
- サーバNIC資源を有効活用、スループット向上が
  見込まれる…はずだった



過去のインライン構成リゾルバVIP構成

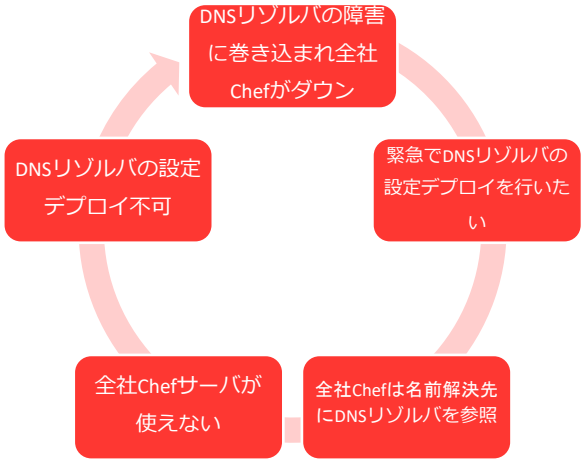
- メリットよりデメリットのほうが大きかった
  - NICの出し分けをサーバ側のStatic Routeで管理
    - Routingが外れることにより通信が吸い込まれる事故
  - 「ここの環境DSRだっけ？インラインだっけ？」という戸惑い・事故誘発



(過去の)ヤフーのDNSリゾルバの問題点(3/3)

全社向けChef Serverを使った構成管理

- DNSチーム以外の管理ツールの障害に巻き込まれるリスクがあった



(過去の)ヤフーのDNSリゾルバの問題点(3/3)

全社向けChef Serverを使った構成管理

- DNSチーム以外の管理ツールの障害に巻き込まれるリスクがあった

→DNSやNTP等、重要なインフラ部位は
全社向けPFとは独立して管理すべき

全社Chefサーバが使えない

全社Chefは名前解決先に社内のDNSリゾルバを参照

過去のヤフーのDNSの問題点まとめ

- サーバの台数が多く、管理・故障対応コストが嵩む
- NW構成がバラバラで管理が大変、事故リスク
- 全社向けPFに構成管理を依存しており、障害発生時のリスク

過去のヤフーのDNSの問題点まとめ

- サーバの台数が多く、管理・故障対応コストが嵩む
- NW構成がバラバラで管理が大変、事故リスク
- 全

対策として各種取り組みを実施

DNSリゾルバ運用コスト削減のために行っている取り組み

扱いやすくする

- DNSリゾルバ構成管理ツールの移行
- DNSリゾルバのリソース最適化
- DNSリゾルバのリプレイスメンテナンス推進

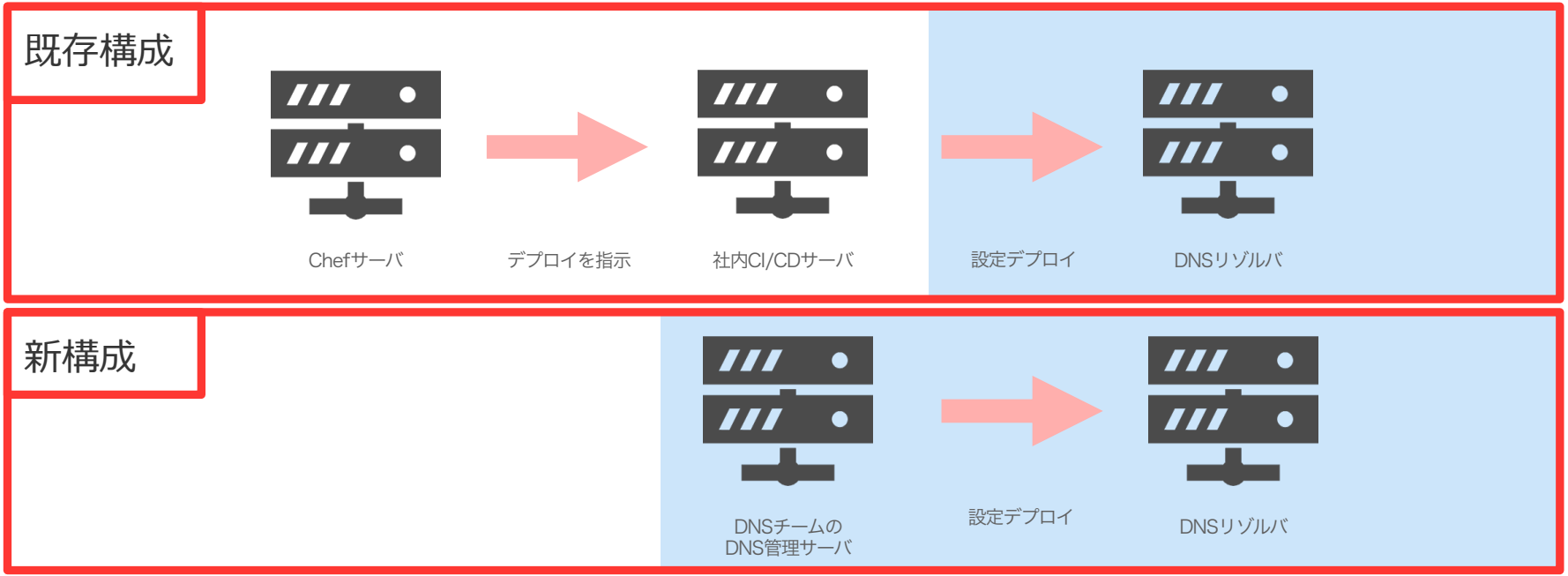
サーバを減らす

- キャッシュDNSアプライアンス導入の開始
- DNSリゾルバのクラスタ統廃合推進

DNSリゾルバ構成管理ツールの移行

- Chefでの管理からAnsibleへの移行を実施

…DNSチーム管轄



DNSリゾルバ構成管理ツールの移行

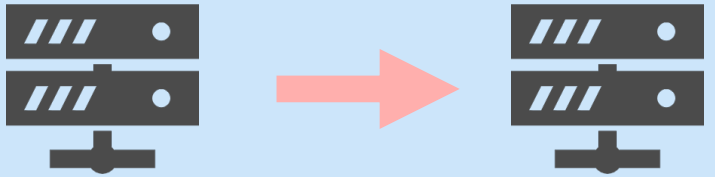
…自チームの管轄

新構成

- 全社PFと切り離すことで障害リスクを軽減
- ネットワーク機器自動化ツールとの親和性

Chefサーバ　デプロイを指示　社内CI/CDサーバ　設定デプロイ　DNSリゾルバ

新構成



DNSリゾルバのリソース最適化

- キャパシティプランニングの再検証
  - 新規環境構築時の負荷見積もりがどんぶり勘定だった
  - 指標とする値が古い時代のサーバでの指標
    - CPUは2世代ほど前、積んだメモリの容量も倍以上違う
  - 現行のサーバでプランニングしなおし、サーバリソースの適正利用

DNSリゾルバのリプレイスメンテナンス推進

- 社内の制約によりメンテナンスウィンドウの確保に難儀
  - キャンペーンなどによるメンテナンス凍結期間
  - DNS関連の別メンテナンスと抱き合わせて実施することにしたが
    その分1回1回のメンテナンスにかかるコストが大きくなる

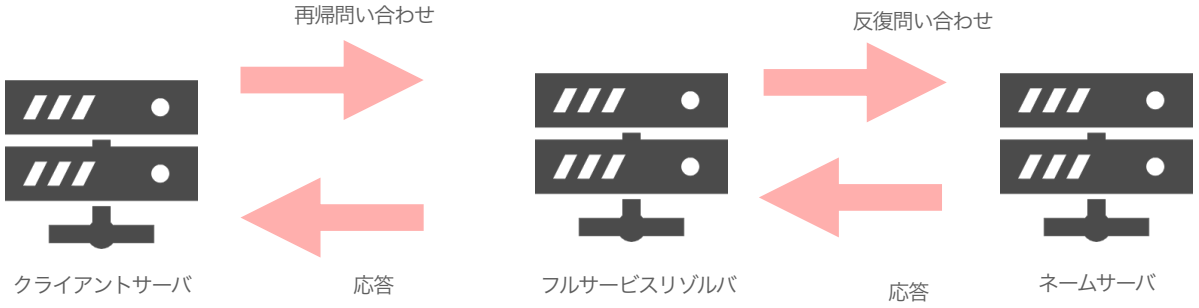
【対策】サービスイン前のサーバ動作確認やロードバランサ側の作業などを自動化

1メンテナンスあたりのコストを削減

キャッシュDNSアプライアンス導入の開始

- 一部の環境でDNSアプライアンスを導入、
  クライアントとリゾルバの間に挟むキャッシュDNSとして利用

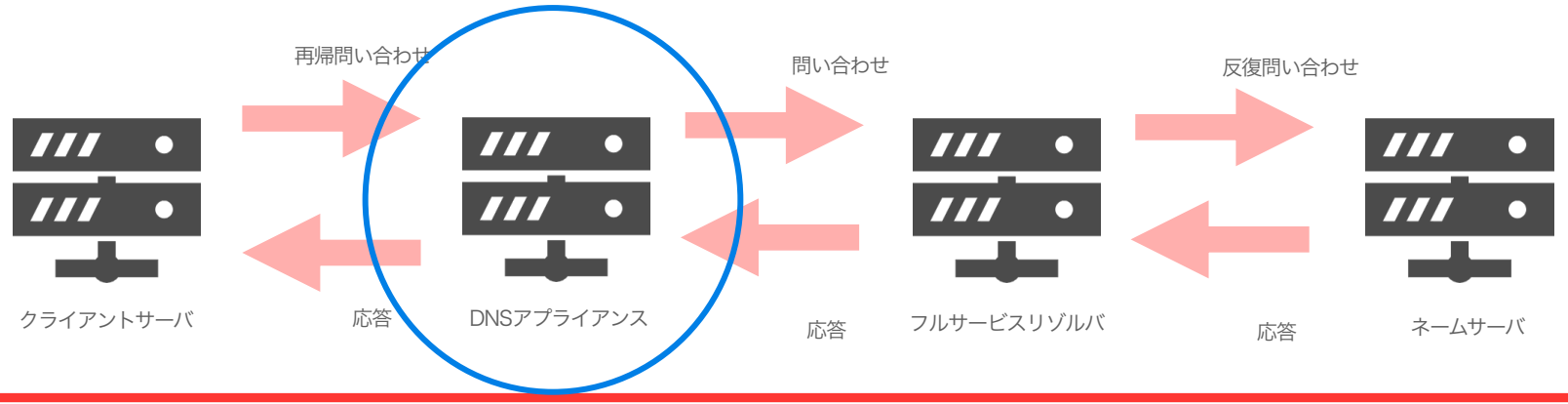
既存構成



- **キャッシュDNSアプライアンス導入の開始**

- 一部の環境でDNSアプライアンスを導入、
  クライアントとDNSリゾルバの間に挟むキャッシュDNSとして利用

新構成



キャッシュDNSアプライアンス導入の開始

- 一部の環境でDNSアプライアンスを導入、
  クライアントとDNSリゾルバの間に挟むキャッシュDNSとして利用
  - BINDとのレスポンス差分をなくすため
- サーバの台数を減らす
- BINDの脆弱性を受けにくくする

DNSリゾルバのクラスタ統廃合推進

- 老朽化したDNSリゾルバのクラスタ統廃合を実施
- クライアント側のresolv.confをDNS運用者側で書き換える
- 社内ツールでresolv.conf書き換え自体は一括で行えるが、懸念事項多数
  - クライアント～新クラスタ間のACLは開いているか？
  - アプリケーションによるresolv.confのキャッシュはされていないか？

DNSリゾルバのクラスタ統廃合推進

半年前
- クライアント側のACLやrouteの設定を確認するよう全社ヒアリング
- メンテナンスの周知

1~2ヶ月前
- 全対象を数回に分け、resolv.confの一括書き換えを実施
- 作業前後の新旧クラスタ宛通信量推移を注視

旧クラスタ停止
- 週ごとに旧クラスタのクエリログ集計・追い出し
- アプリケーション・サーバ再起動を促す

DNSリゾルバのクラスタ統廃合推進

- クライアント側のACLやrouteの設定を確認するよう全社ヒアリング

最終的に売上毀損無しでの旧クラスタ停止を完遂

旧クラスタ停止

- アプリケーション・サーバ再起動を促す

取り組みによる運用改善結果

設定変更作業に伴うデプロイ工数削減

- 約半日→1,2時間へ

DNSリゾルバの台数削減

- 300台程度→200台程度

サーバ故障率の低下

- 2019年、2022年のHDD/メモリ故障などによる筐体調査回数を集計
- 19年→22年で筐体調査回数が約1/10に激減

今後の運用改善展望

- Ansible Deployの自動化
  - named.confのファイルを弄っておけば勝手に反映される
- キャパシティプランニング結果に基づくサーバリソースのさらなる最適化
- Anycastなど、新たな構成の検討

皆様の所属先ではDNSリゾルバ運用コスト削減のため
どのような取り組みを行っているかぜひご教示ください

まとめ

- ヤフーでは大量のDNSリゾルバを運用しており、
  運用コストがチームの負荷になっていた
- サーバ台数削減、管理ツールの移行など様々な方向からの
  コストの削減を進めている