

KDDIにおけるLBレス事例の共有

KDDI株式会社

January 27, 2022



Agenda

■ はじめに

- 自己紹介
- 今回の内容

■ 事例紹介

- 事例1
 - OSPFによる分散
- 事例2
 - StaticRouteの2重書きによる分散

はじめに

■ 自己紹介

● 名前

- ・ 松本 章(まつもと あきら)

● 所属

- ・ KDDI株式会社 プラットフォームエンジニアリング部

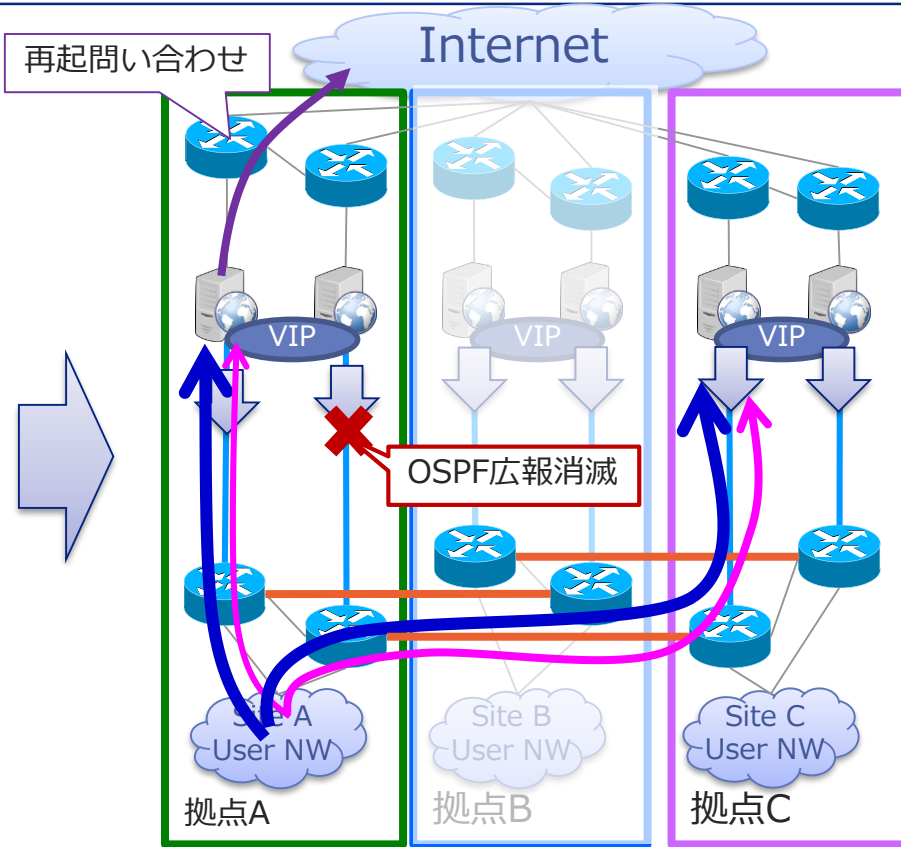
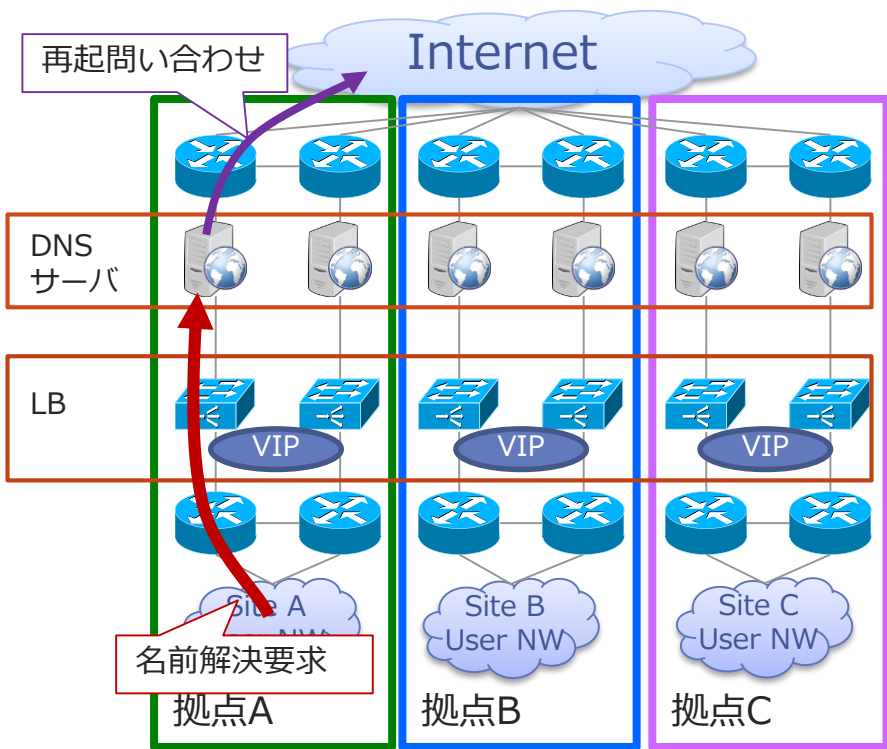
● 仕事

- ・ 事業用のDNS/NTPのシステム設計構築と運用支援

■ 今回の内容

- **ISPでのロードバランサ(以下、LB)を使用しない複数台DNSサーバの導入事例の共有。**

事例1(Before/After)

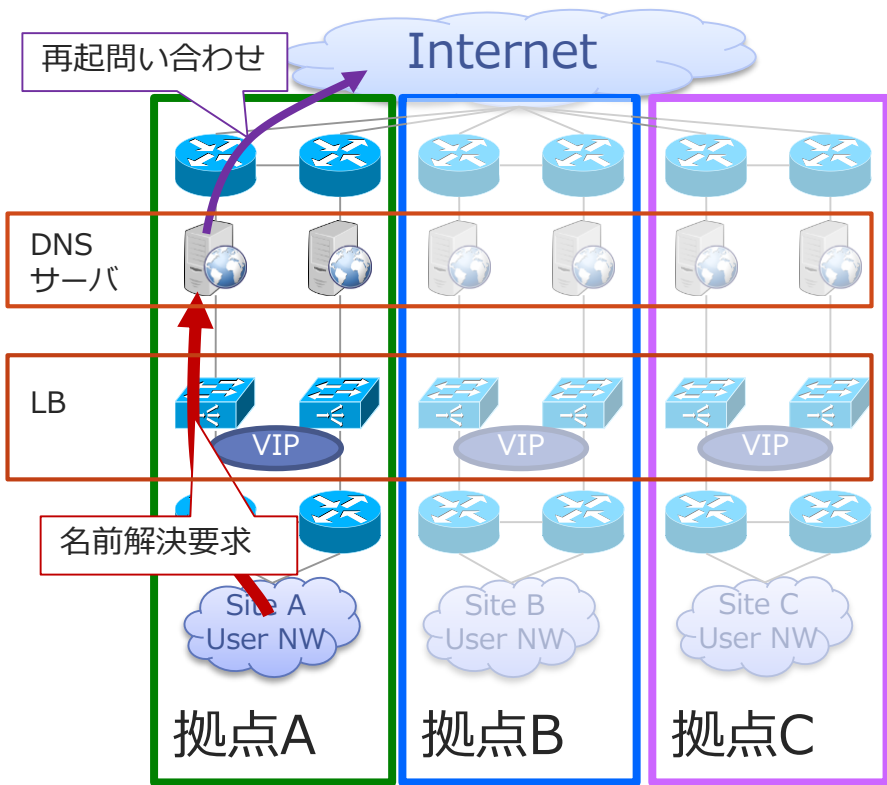


VIP

サービスVIP(IPv4x2IP)
Primary/Secondaryを各拠点で同一IPで付与。

※DNSサーバは2台がP/S両方を広報。

事例1(Before)

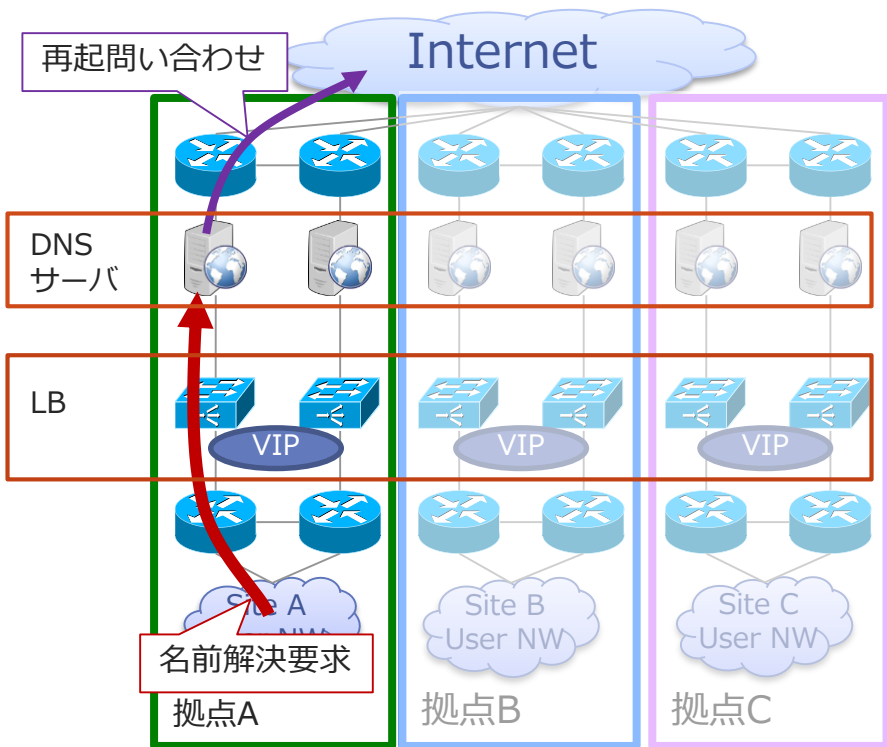


NWの状況

- 拠点A/B/Cの3拠点にDNSサーバが独立して存在。
- サービスVIPをLBに付与。
- 各拠点のUser NW内にいるお客様はUser NWからVIP宛にDNS問い合わせ。
- ユーザは同一拠点のDNSサーバのみを利用可能。

※図を見やすくするため、説明箇所以外の拠点を網掛けしております。

事例1(Before)



抱えていた課題

- DNSサーバ/LB共に著しく老朽化
- 拠点間が独立しており、BCP/DRに課題。
- LB更改が困難
 - ・ 「LBの予算は計上していない」。

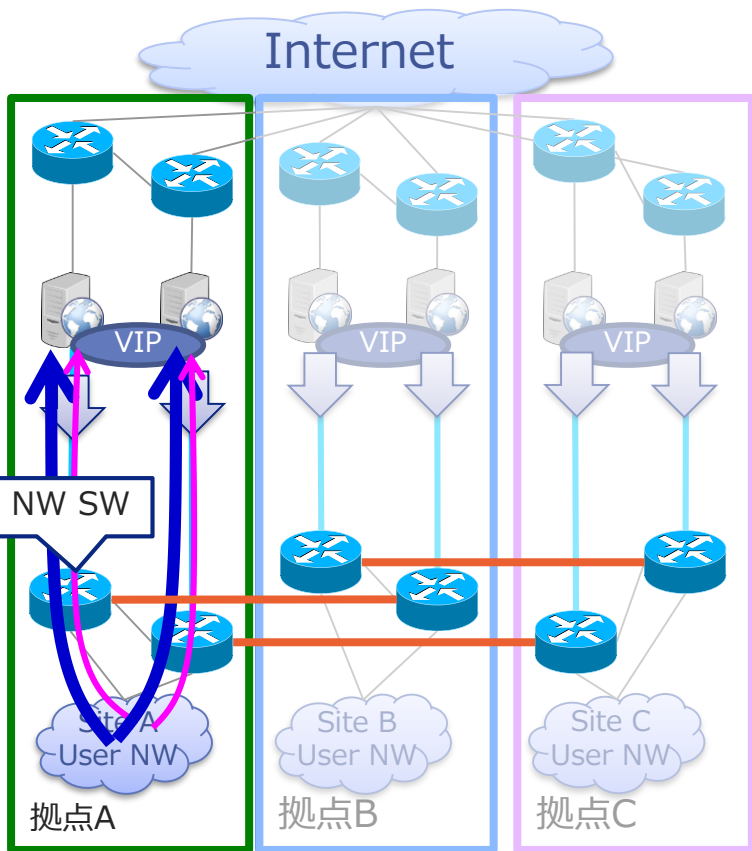
VIP

サービスVIP(IPv4x2IP)

Primary/Secondaryを各拠点で同一IPで付与。

※図を見やすくするため、説明を行わない拠点は薄くしています。

事例1(After)

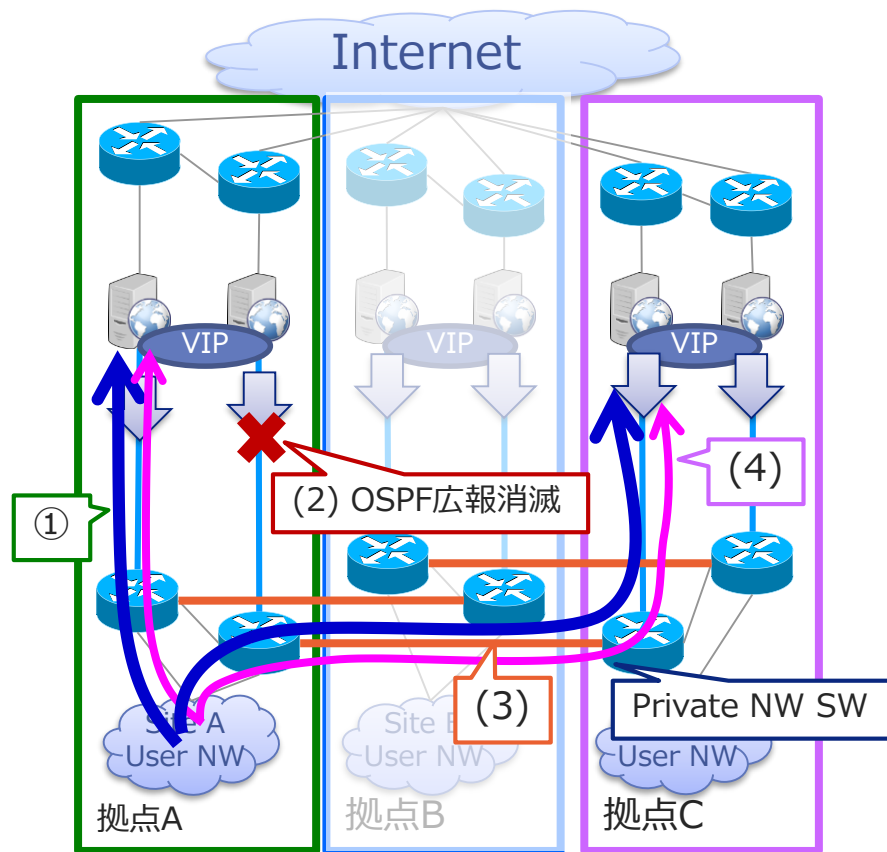


※DNSサーバは2台ともP/S両方のサービスVIPを広報。

改善の内容

- LBを撤去。
- 拠点間のPrivate NW SW同士を接続(橙線)。
- DNSサーバがサービスVIPをOSPFでPrivate NW SWに向けて広報(↓矢印)。
 - 2台が2台ともP/S両方を広報
- Private NW SWはサービスVIPをUser NWに向けて再広報。

事例1(After)



※DNSサーバは2台ともP/S両方のサービスVIPを広報。

改善後のフロー

- 通常時はユーザは水色線経由で同一拠点のDNSサーバへアクセス(1)。
- 拠点AのDNSサーバが落ちると、DNSサーバからのOSPF広報が停止(2)。
- 拠点AのPrivate NW SWは、橙色線経由の経路を使用開始(3)。
- 拠点Aのユーザは橙色線経由で拠点CのDNSサーバを使用開始(4)。
- これにより、LBレスによる分散を実現(拠点間でも実現)。

実施してみてもの良かったところと問題点(事例1)

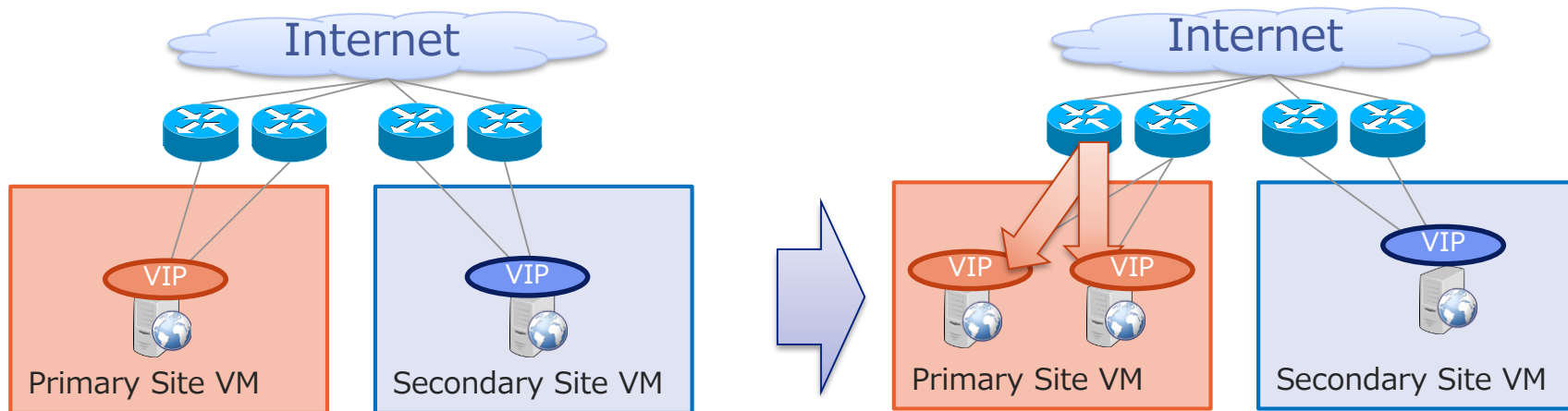
■ 良かったところ

- LBを購入せずに拠点内トラフィック分散を実現。
- OSPFをうまく使って拠点間分散も実現。

■ 問題点

- 製品依存がある/設定が複雑。
 - OSPFを喋れるサーバが必要。

事例2(Before/After)



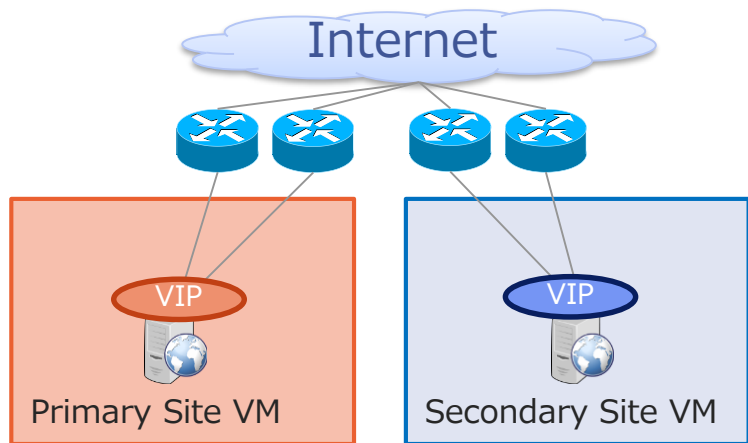
サービスVIP

(橙/左: Primary, 青/右: Secondary)



事例2

■ Primary/Secondary 1台構成



- 仮想環境でPrimary、Secondaryをそれぞれ1台でお客様向けにフルリゾルバを提供。
- HTTPSレコード(Type65)の増加によりPrimaryのサーバが性能不足が顕著化。
 - ・ P/S片方が落ちるとトラフィックが溢れる。
 - ・ なぜ予想できなかったのか？と詰められる。
- KDDIとしてDNSで仮想LBは未導入な上、超短納期増設が求められる状況。
 - ・ 巻取先はあったが構築に時間を要する状況。

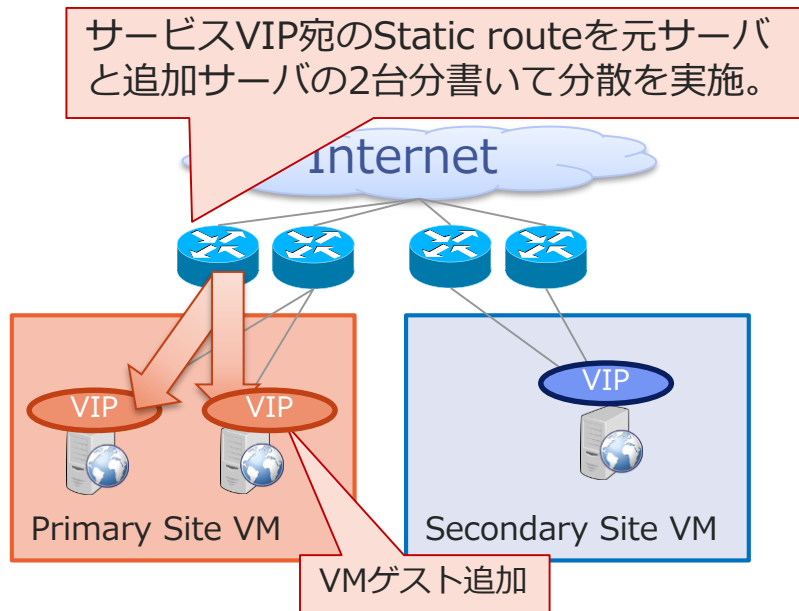
サービスVIP

(橙/左: Primary, 青/右: Secondary)

※現在は本構成ではありません。

事例2

■ PrimaryのみLBレス等コスト分散



- まずは性能不足が顕著だったPrimary SiteにDNSサーバ(VMゲスト)を増設。
- 増設後、上位ルータにDNSサーバ向けのStatic Routeを追加。
- 追加後、LBレスで2台のDNSサーバにトラフィックが等分散されることを確認。

【イメージ】

```
ip route サービスVIP 255.255.255.255 <元のサーバ>  
ip route サービスVIP 255.255.255.255 <追加サーバ>
```

※現在は本構成ではありません。

LB構成と比較した差分 (事例2)

■ 良かったところ

- 短納期かつ安価に増設を実現。
- 全体的に見るとトラヒックの均等分散を実現。

■ LB構成と比較した差分

- DNSの生死に関わらずトラヒックを振られる。
- 均等分散を前提とした構成になる。
 - ・ 分散先サーバの性能が同一か、性能差が小さいことが前提。
- TCP SYN CookieやRateLimit等はサーバ側で実装が必要。
- 個々のSource IP単位で見ると分散されてない。

まとめ

■ LBレス構成によるメリット

- LBが不要になるため安価
 - ・ LBを「等分散するためだけ」に設置しているのであれば検討の価値あり。
- 設定が容易(Static Routeの場合)

■ LBレス構成による課題

- LBと「同等機能」は期待できない。
 - ・ DNSサービス停止時に自動的に切り離す機構が必要。
 - LBであればHealth Check機能でサービス無応答時に自動閉塞可能。
 - ・ Soft Start不可
 - 大規模なキャッシュDNSに耐えうるかは疑問。

免責

■ 免責事項

- **記載事項について正確性や再現性を保証するものではありません。**
 - ・ 不具合等が発生した場合においても弊社(私含め)は一切の責任を負いかねます。あらかじめご了承ください。
 - ・ なお、構成図はいずれもシンプル化しています。
- **LBの導入または非導入のいずれも推奨するものではありません。**

Tomorrow, Together

