フルサービスリゾルバのアウトソース化について(事前資料)

JANOG51 Meeting in Fujiyoshida

2023年1月20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サービス部
其田 学

ISPのフルサービスリゾルバ（フルリゾルバ/キャッシュDNSサーバ)を アウトソースし外部サービスを利用する際に、どのような考慮が必要か考える

今回のお題に至った背景

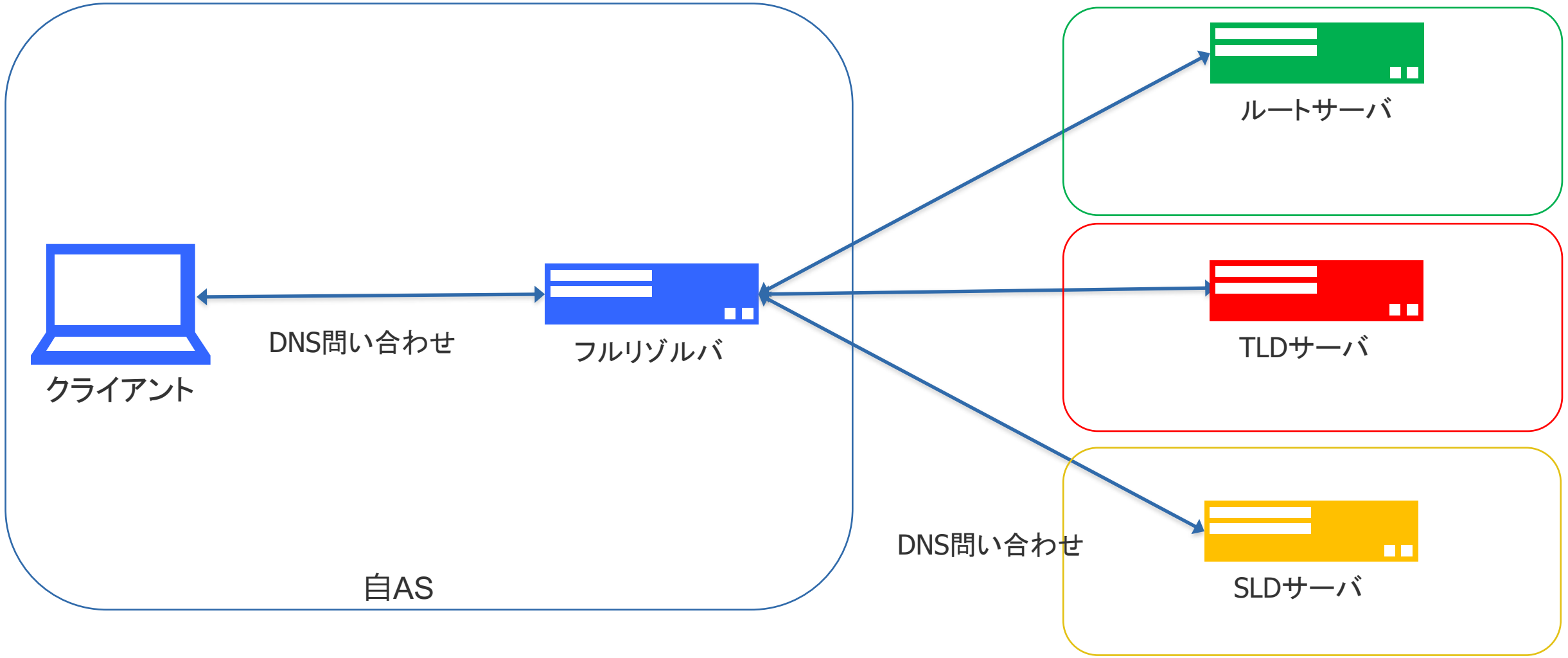
フルサービスリゾルバをアウトソースしたいという相談が増えている（IIJでは）

フルサービスリゾルバが提供する名前解決は通信の一部なので、メールやWEBサービスといった、アプリケーションサービスとは違う考慮が必要

フルサービスリゾルバとは

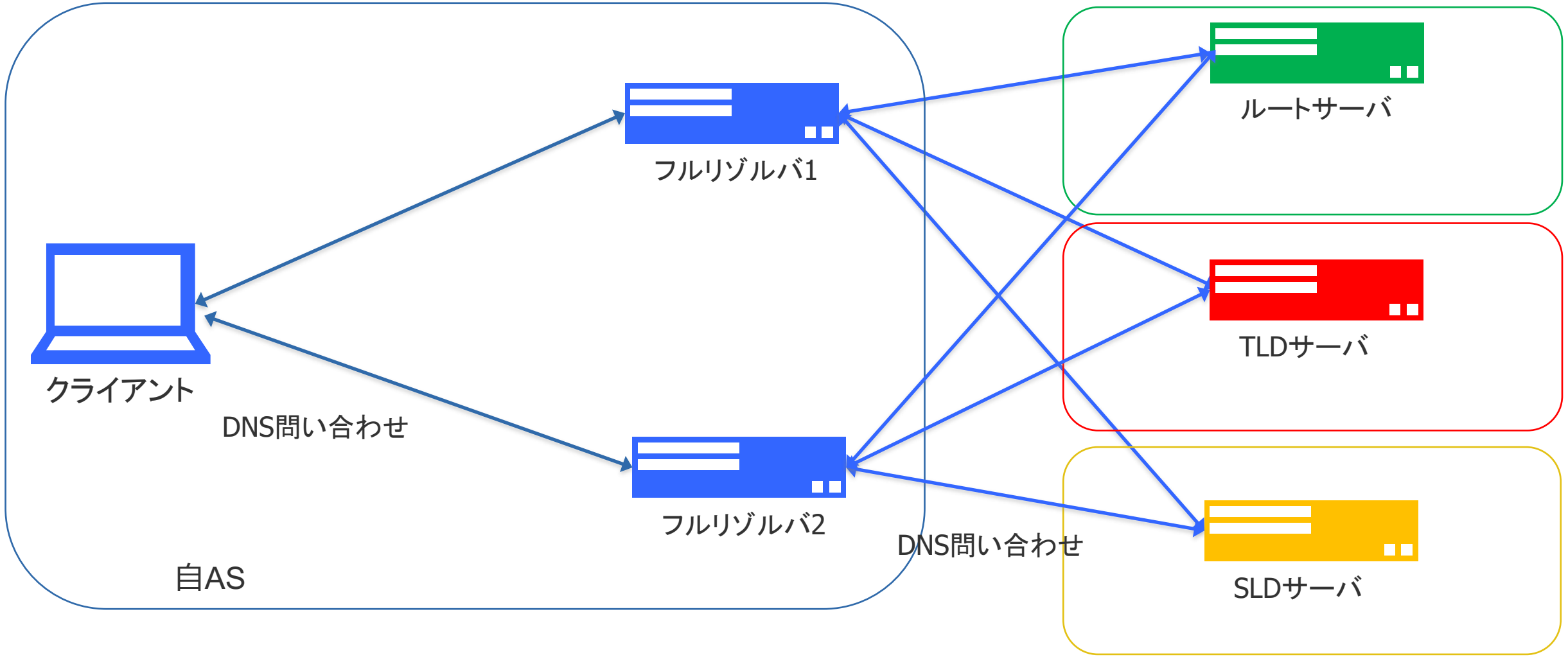
フルサービスリゾルバとは

クライアント(スタブリゾルバ）からの問い合わせを受けて、ルートサーバから順に、権威DNSサーバに問い合わせを行い名前解決を行い、得られた結果をクライアントに返すサーバ。結果をキャッシュして答えるので、一般にキャッシュDNSサーバと呼ばれる



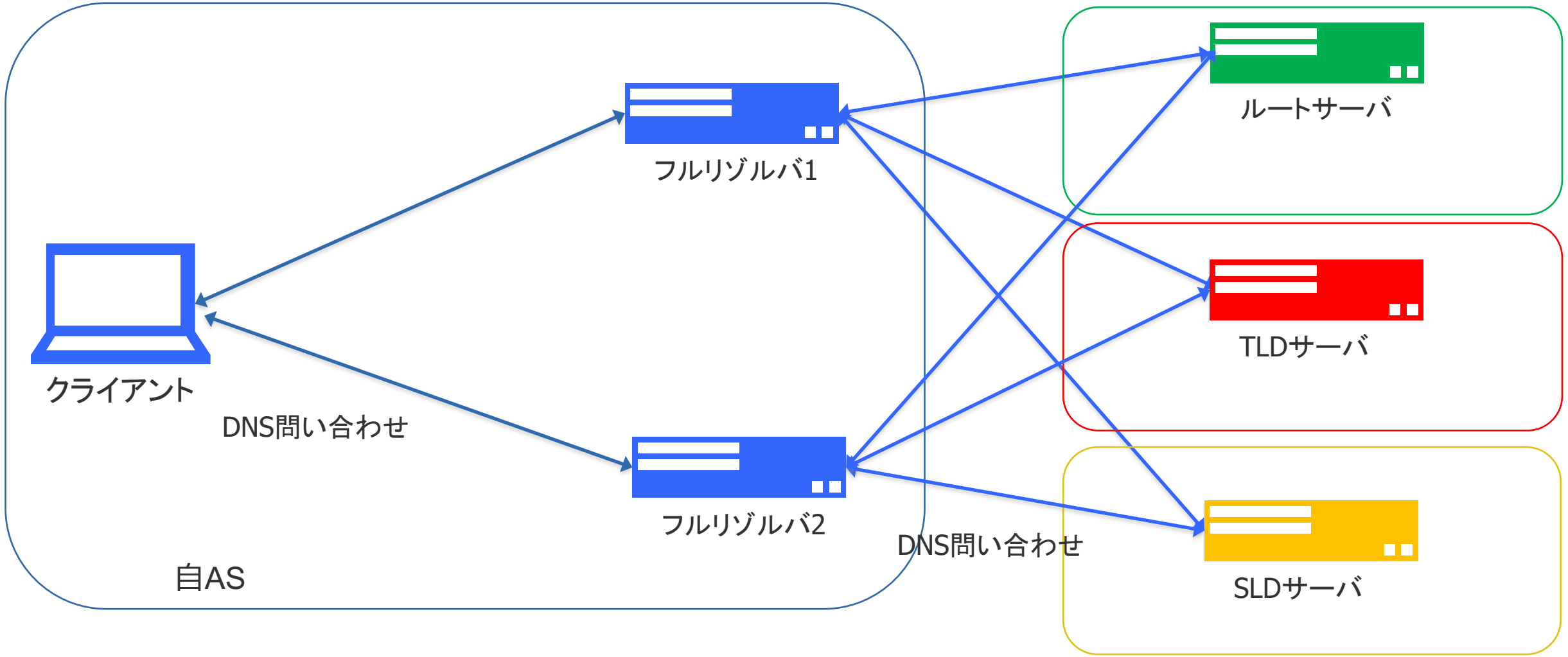
フルサービスリゾルバとは – 冗長構成

クライアントは複数のフルサービスリゾルバの設定を持つことができる。これにより冗長構成がとれる
通常ISPでは２系統以上のフルサービスリゾルバを提供しており、１系統が障害になっても致命的な影響がないようになっている



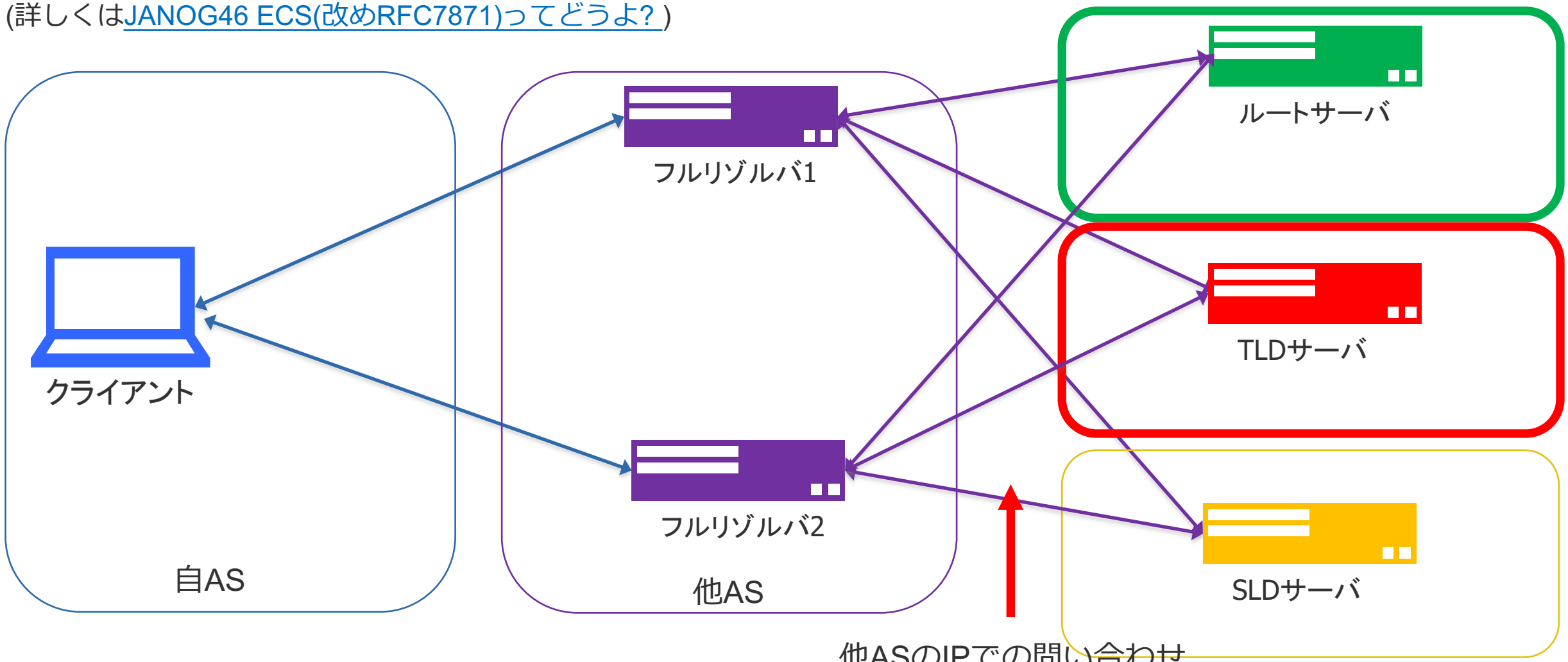
フルサービスリゾルバとは – 最適応答

権威DNSサーバはフルサービスリゾルバのIPアドレスがわかるため、DNSベースのCDNなどは、そのASに最適な返答を行うことがある。例えばCDNの権威DNSサーバは、NW的に近いサーバ（例えばISP内のコンテンツキャッシュサーバ）を返答したりする



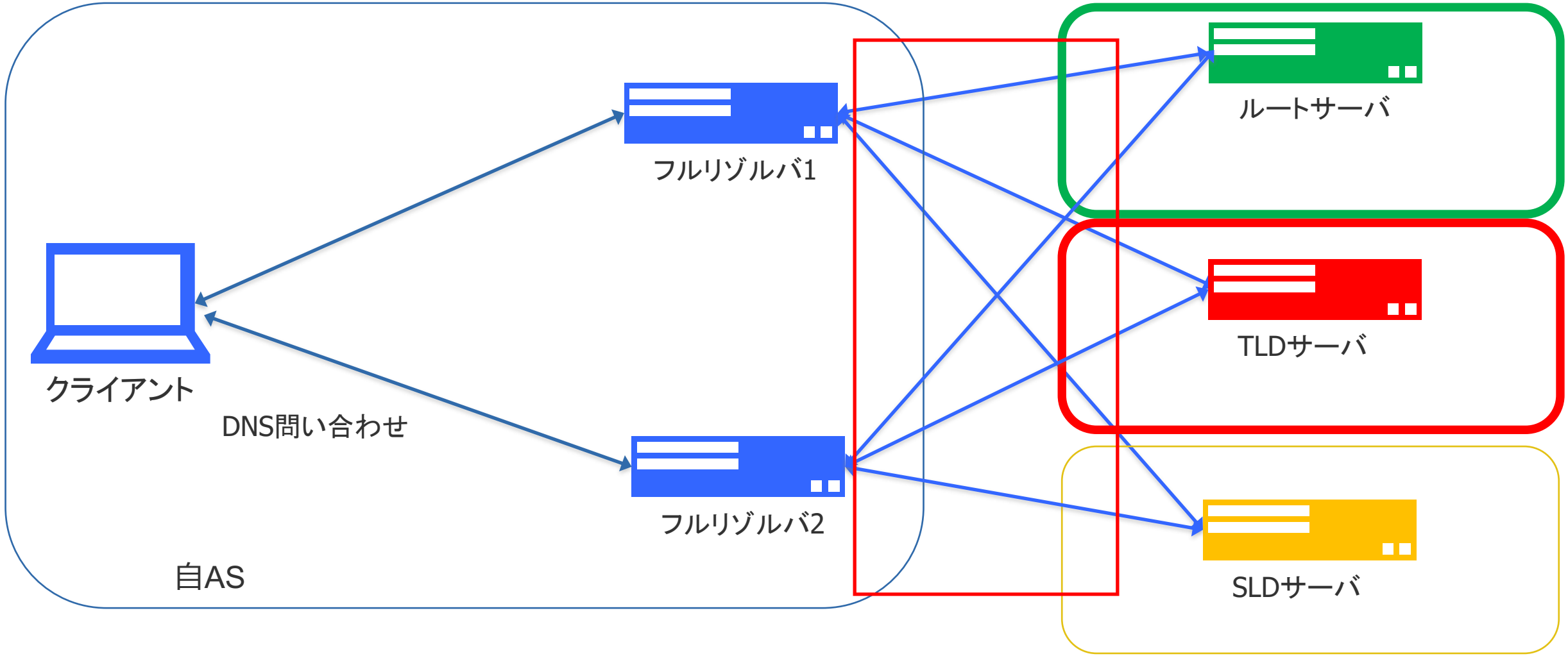
フルサービスリゾルバとは – 最適応答 - ECS

フルリゾルバを外部ASにアウトソースすると、自ASに最適な応答を得られない可能性がある
また、クライアントがPublic DNS利用でも同様のことが起こる
それを解消するために、フルリゾルバから、権威DNSサーバへの問い合わせ時に、クライアントのIPを
Maskしたソースネットワークを付加するEDNS Client Subnetという機能が追加されている
(詳しくはJANOG46 ECS(改めRFC7871)ってどうよ?)



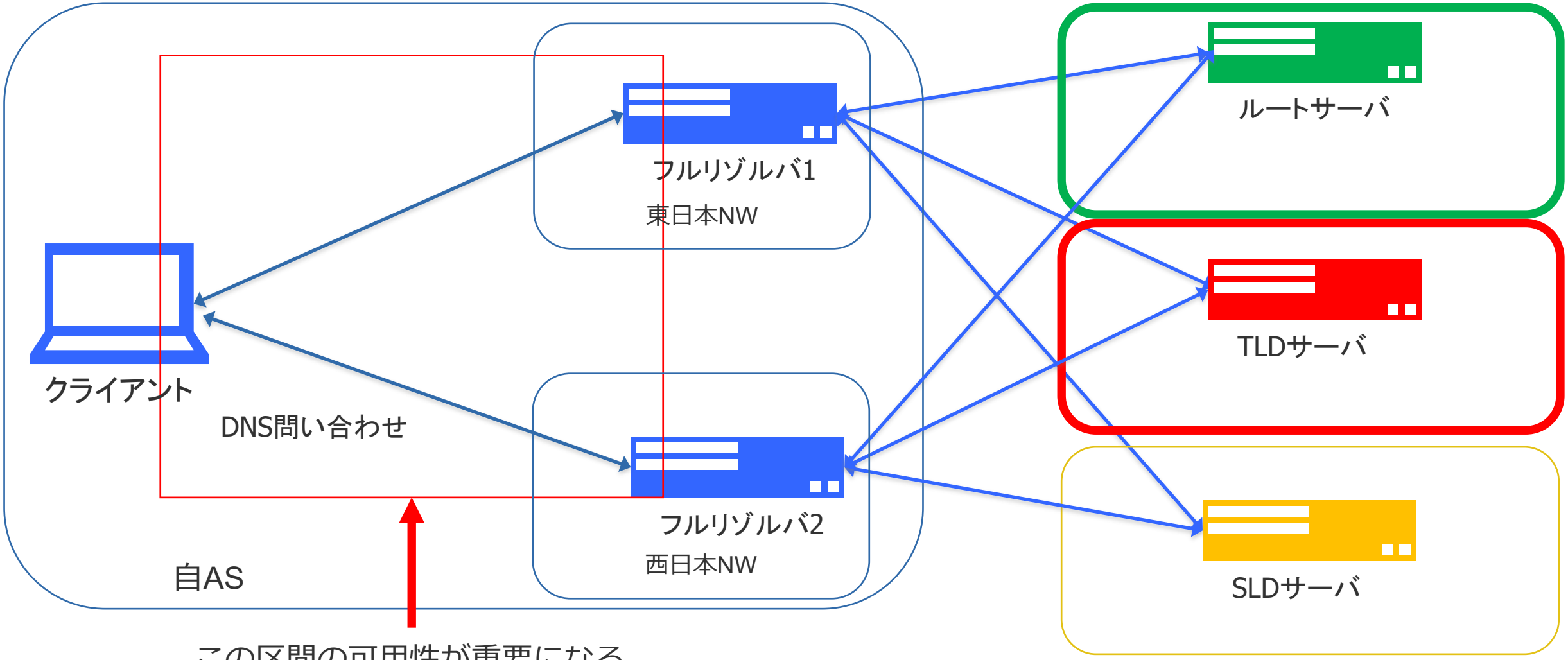
フルサービスリゾルバとは – 可用性

フルリゾルバと権威DNSサーバ間の可用性は、厳密に考えなくても良い
ルートサーバと多くのTLDサーバはIP Anycastかつ、多AS運用しているので、全ての経路が落ちることは考えにくい
SLDサーバは特定ドメイン名しか影響がでないので全断というレベルではない
また、多くの問い合わせがある名前は、キャッシュが残っている場合が多いので、数分程度の停止でも問題がない場合が多い



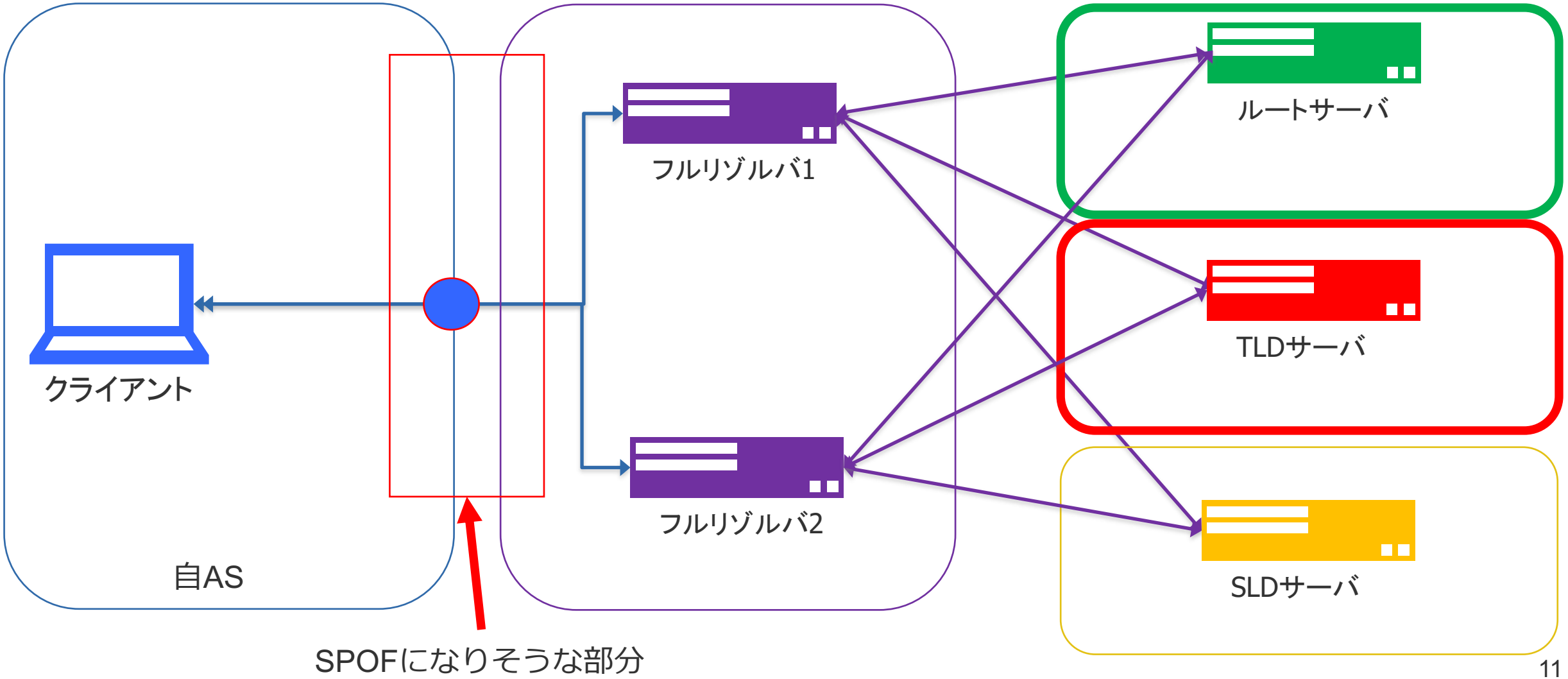
フルサービスリゾルバとは – 可用性

一方で、クライアントとフルリゾルバ間の可用性は重要
クライアント側でキャッシュがない場合もあり、両系が断になると通信が止まる
そのため、系の分離(NW,AZ,Location)を行ったり、LBやAnycastなどで可用性を高めている



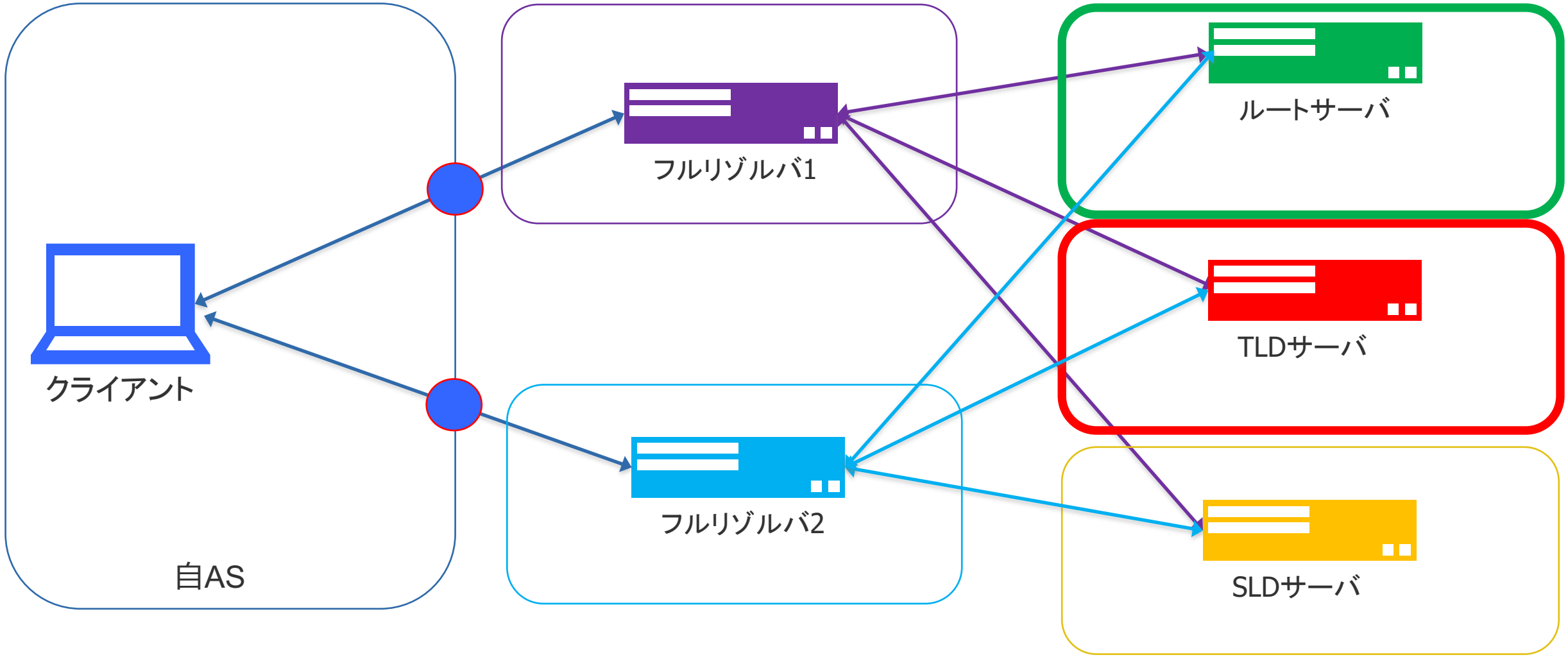
フルサービスリゾルバとは – アウトソース時の可用性

一つのフルリゾルバサービスを設定した場合、フルリゾルバサービスのAS内でNW的な冗長性がとられていても、
接続部分がSPOFになる可能性がある



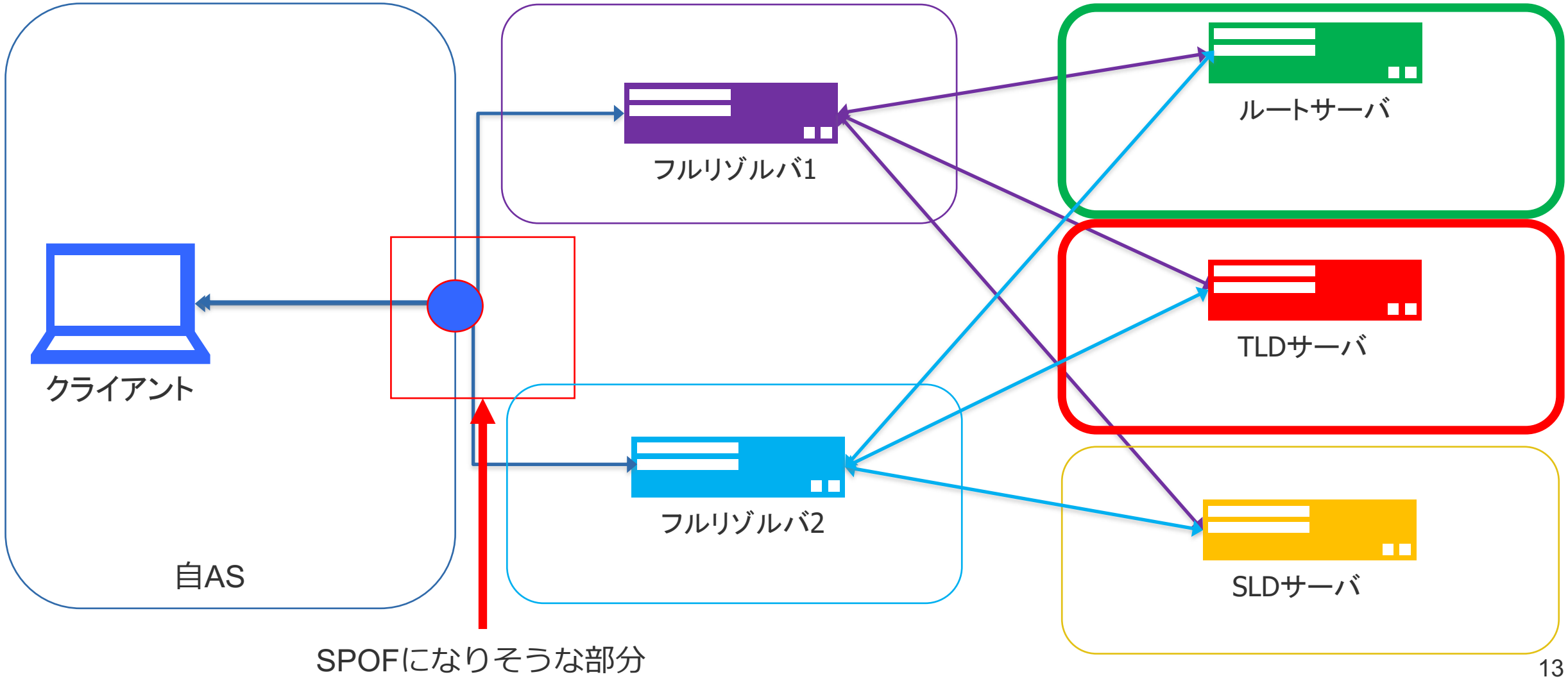
フルサービスリゾルバとは – アウトソース時の可用性

複数のフルリゾルバサービスを設定した場合は、一つの場合に比べるとSPOFにはなりにくい
ただ、同じIXで接続していたり、同じトランジットを通っていたり、同じルータに収容している可能性はある



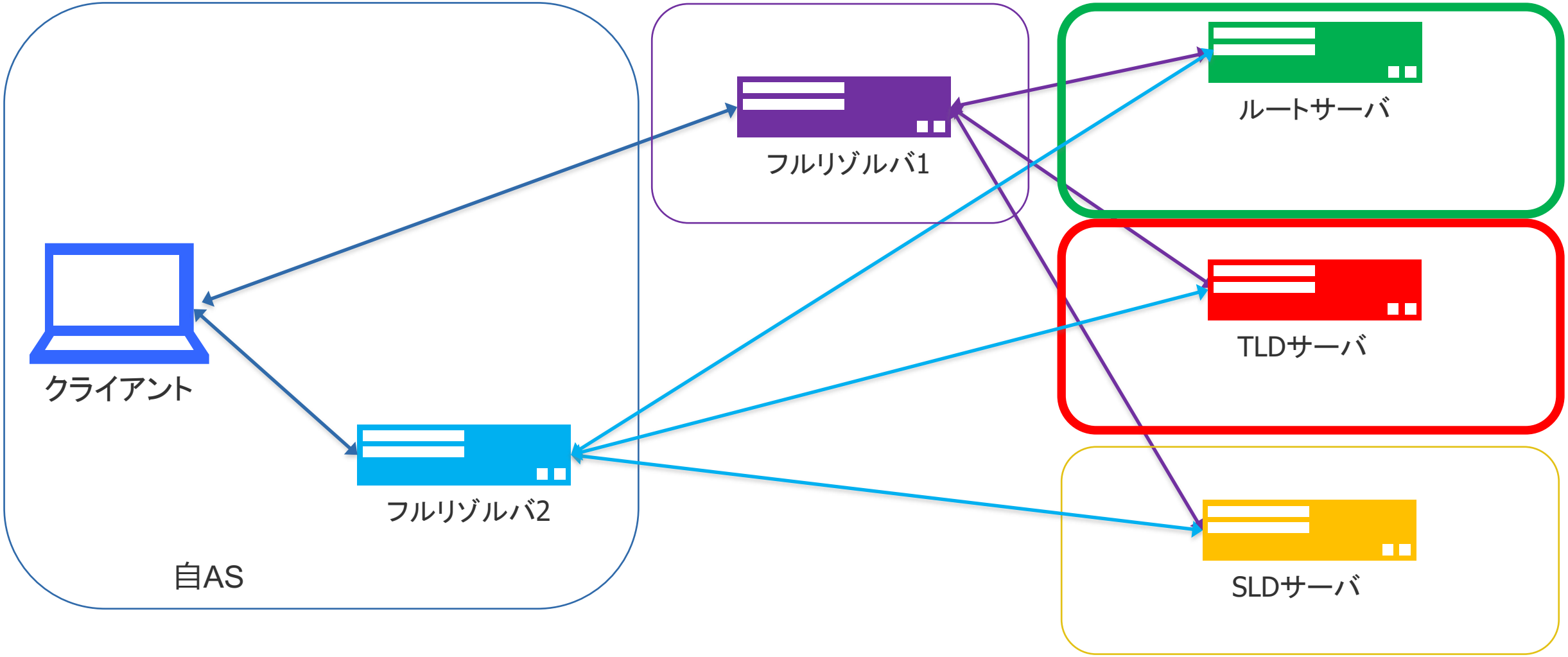
フルサービスリゾルバとは – アウトソース時の可用性

複数のフルリゾルバサービスを設定した場合は、一つの場合に比べるとSPOFにはなりにくい
ただ、同じIXで接続していたり、同じトランジットを通っていたり、同じルータに収容している可能性はある



フルサービスリゾルバとは – アウトソース時の可用性

複数系統の一部だけ、アウトソースする方法もある
この場合は、片系は自ASに残るので、自AS内の経路や、収容ルータの調整でSPOFは少なくできる



フルリゾルバをアウトソースするモチベーション

相談を受けたISPの規模や考え方によって、モチベーションは様々

1. コスト化したい
- メールもWebも認証もBGP運用も全部アウトソースしたい（している）
- DNSもその流れでアウトソースしたい

2. 運用負荷を減らしたい
- リプレース機材の削減

3. 冗長性の向上
- 片系を別実装のフルリゾルバサービスにすることで、ゼロデイ攻撃を緩和したい

フルリゾルバをアウトソースする上での観点

当日おもに話したいのはこの３点

1. プライバシー
2. 可用性
3. 契約面

1. 名前解決は通信の一部と見做されている

- フルリゾルバ上のクエリログは通信ログに他ならない
- クエリログの保存などはフルリゾルバサービス提供者のポリシーに従うことになる
- どのような、ポリシーがフルリゾルバサービスに必要か

2. ECSのプライバシー問題

- アウトソース前は、権威DNSサーバは、フルリゾルバのIPのみ見えていた
- ECSを有効にすると、権威DNS側は、 クライアントのネットワークがわかってしまう
  - エンドユーザの通信先が、権威DNSサーバ側にある程度わかってしまう可能性
  - 特に大規模なDNSプロバイダの場合はより多くの情報を収集できる
  - Cloudflare(1.1.1.1)のように実装しないPublic DNSもある
- 問題を軽減するために、どれぐらいのMASK値が良いのか
  - 大きすぎると、割り当てCIDRを超えてしまう可能性
  - 細かすぎると、プライバシー面への悪影響

1. **フルリゾルバサービス自体の可用性**
   - サービスのSLAに基づいて考えれば良い
   - 共用サービスなので、他者の影響を受ける可能性がある
     - 他のISPがDNSリフレクター攻撃を受けた場合など
   - そのような事態を想定して作られているので、全ユーザに影響が出るような障害は自前より少ないはず
     - Rate Limit等のセキュリティ機構がエンドユーザの名前解決を止める可能性はある

1. **クライアントと、フルリゾルバサービス間の可用性**
   - フルリゾルバサービスとの直接接続ができない限り、可用性は下がる
   - 当たり前だが、接続形態で不確実性が上がる
     - Private peer < IX接続 < トランジット経由
     - Private peer以外だと、第３者のトラフィックに巻き込まれる可能性も高い
   - 最適な利用形態はどのようなかたちなのか

ISPとしてフルリゾルバの提供をやめる場合

- 多くのISPがNTPを提供しなくなったように「ISPではフルリゾルバは提供しません、自前で立てるか、Public DNSの利用を推奨します」みたいなこともできる
  - 法人回線などでは普通にある
- この場合は提供してないので、考慮することはない

ISPがフルリゾルバサービスを調達して提供している場合

- 単に運用を外部に出しているだけで、エンドユーザからみてフルリゾルバの提供者はISP
- ISPがフルリゾルバサービスの利用規約、約款に同意する必要がある
- フルリゾルバサービスで、DNSフィルタリングが導入されていて、外せない場合、通信の秘密を侵すので、ユーザの同意が必要

ISPがPublic DNSをユーザに指定する場合

- ISPがPublic DNSを指定することがPublic DNS的に認められるのか
  - Google Public DNS for ISPとかもあるんで、認められそう
- エンドユーザがPublic DNSの利用規約に同意する必要がある
  - DHCPやIPCPで配る場合、ISPが配っているので、どうやって同意をとるのか

続きはJANOG51で

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。