フルサービスリゾルバのアウトソース化について(発表資料)

JANOG51 Meeting in Fujiyoshida

2023年1月26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

名前

其田 学

所属

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DNS技術課

経歴

- 2014年から、IIJのDNSサービスの運用に従事
- それ以前は別のISPで、ネットワーク運用業務に従事
  - バックボーン運用とか、VPNサービス運用やってました。

今回のお題

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

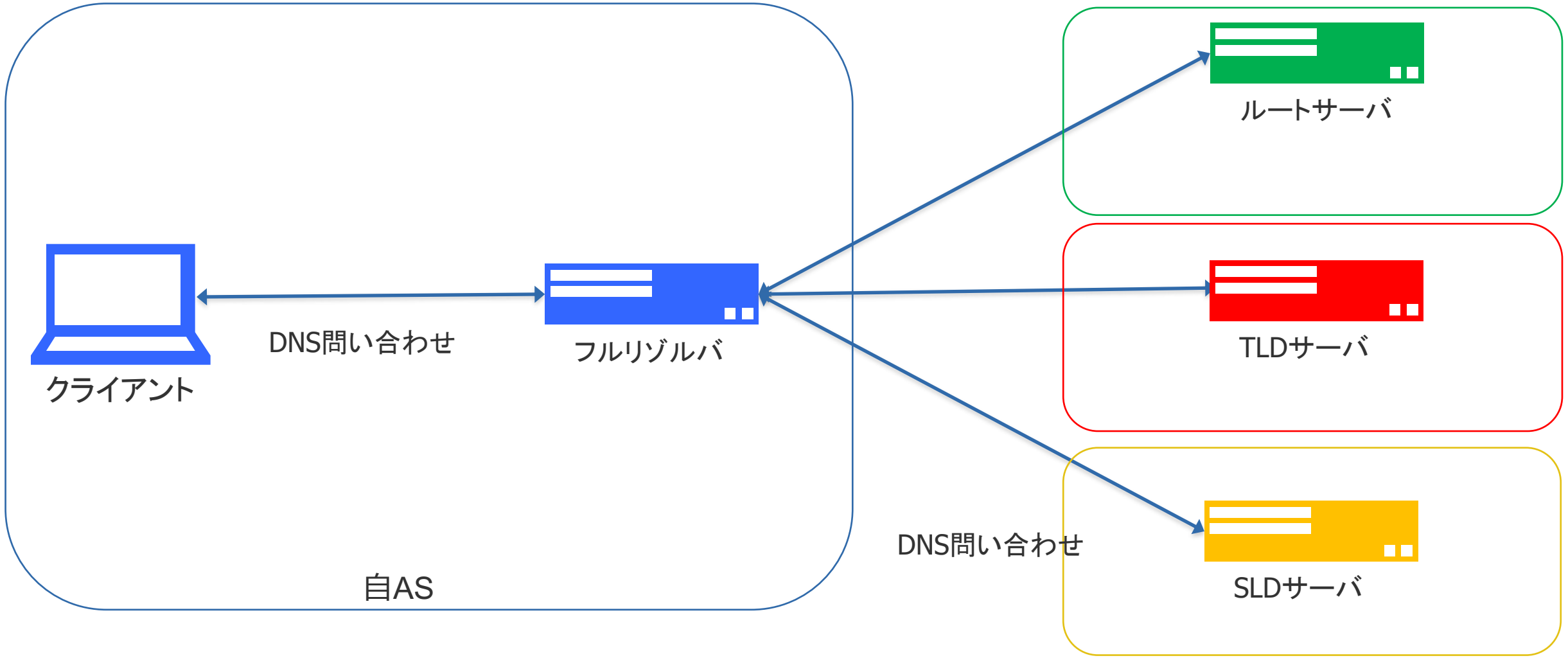
2. 運用負荷を減らしたい
- リプレース機材の削減

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

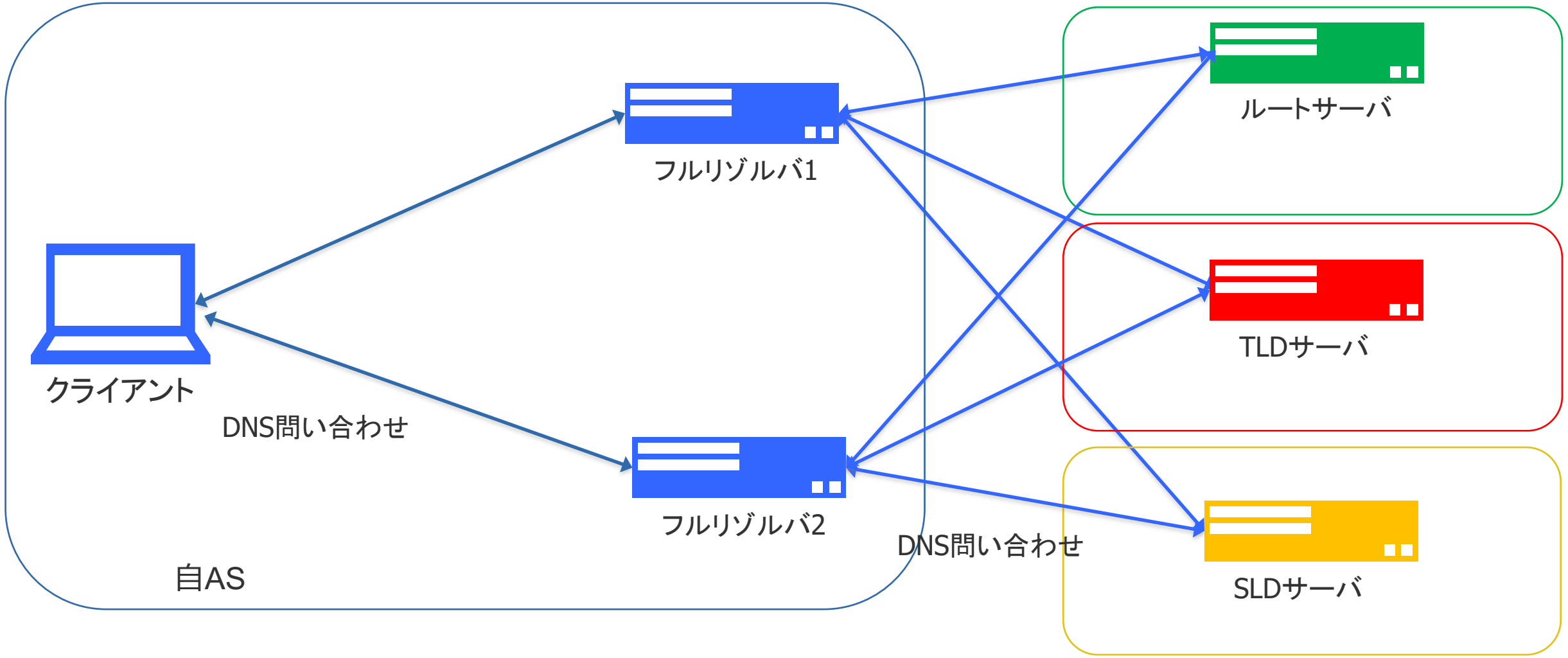
フルサービスリゾルバとは

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



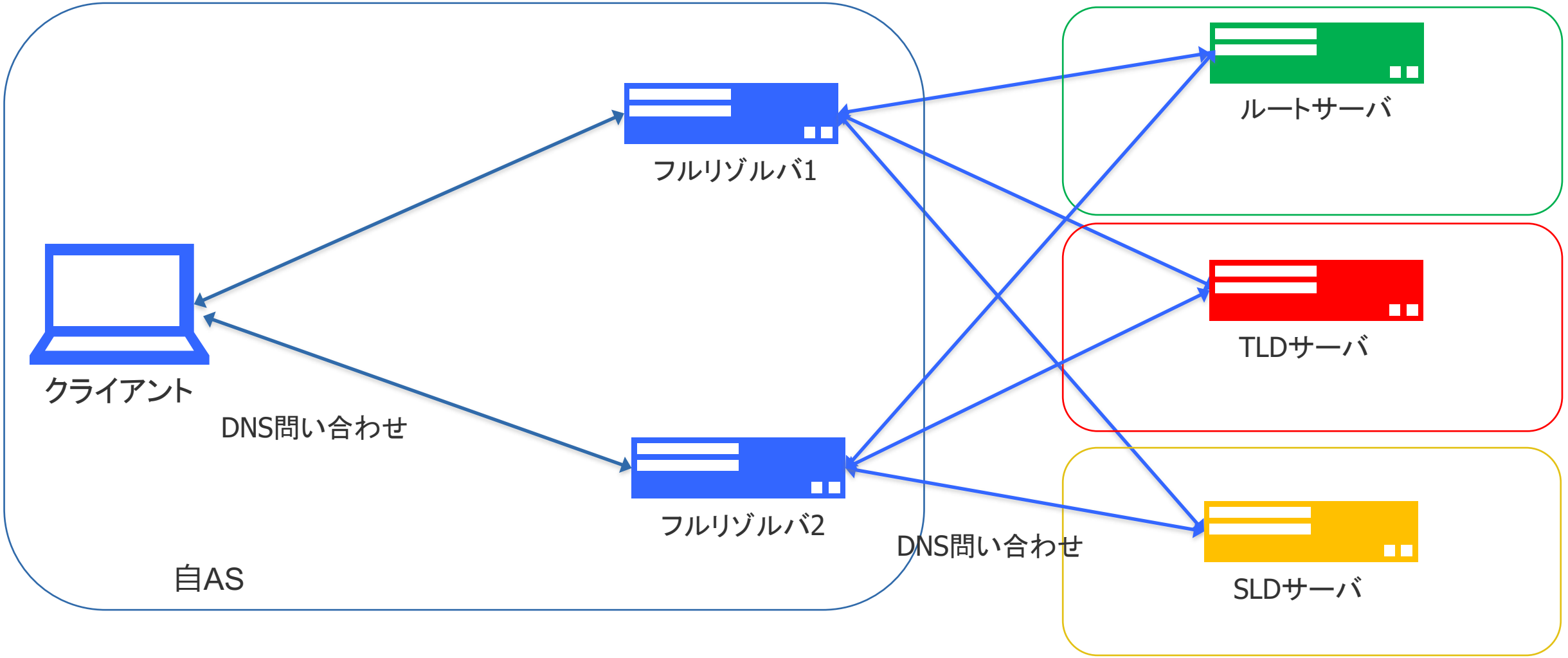
フルサービスリゾルバとは – 冗長構成

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



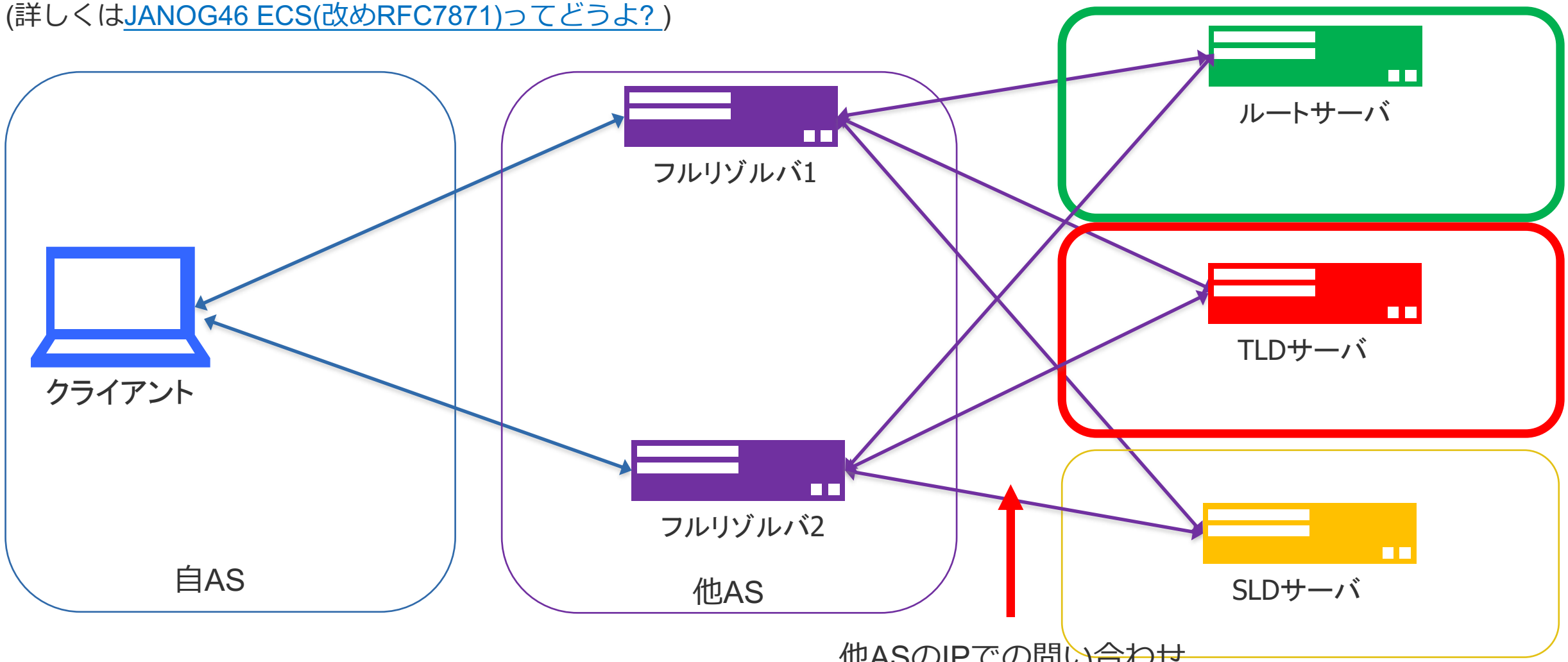
フルサービスリゾルバとは – 最適応答

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



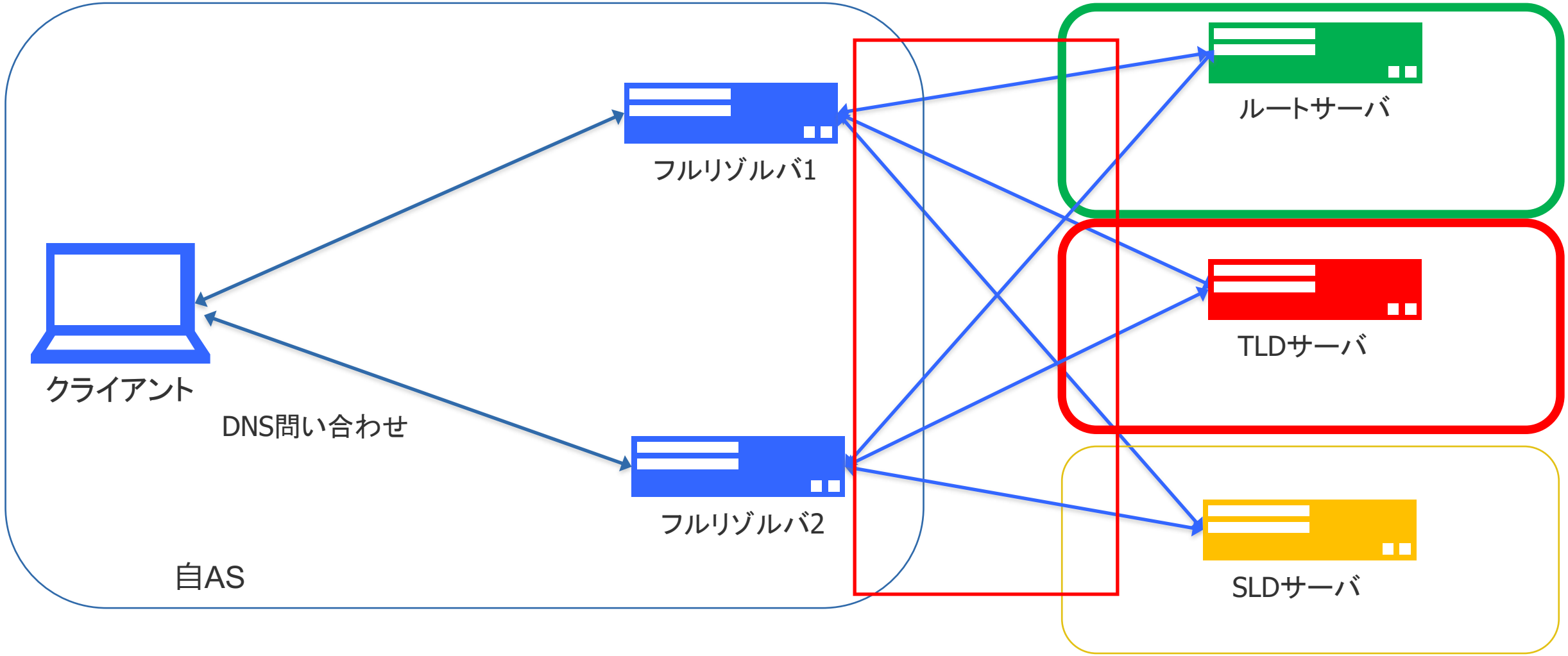
フルサービスリゾルバとは – 最適応答 - ECS

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?)



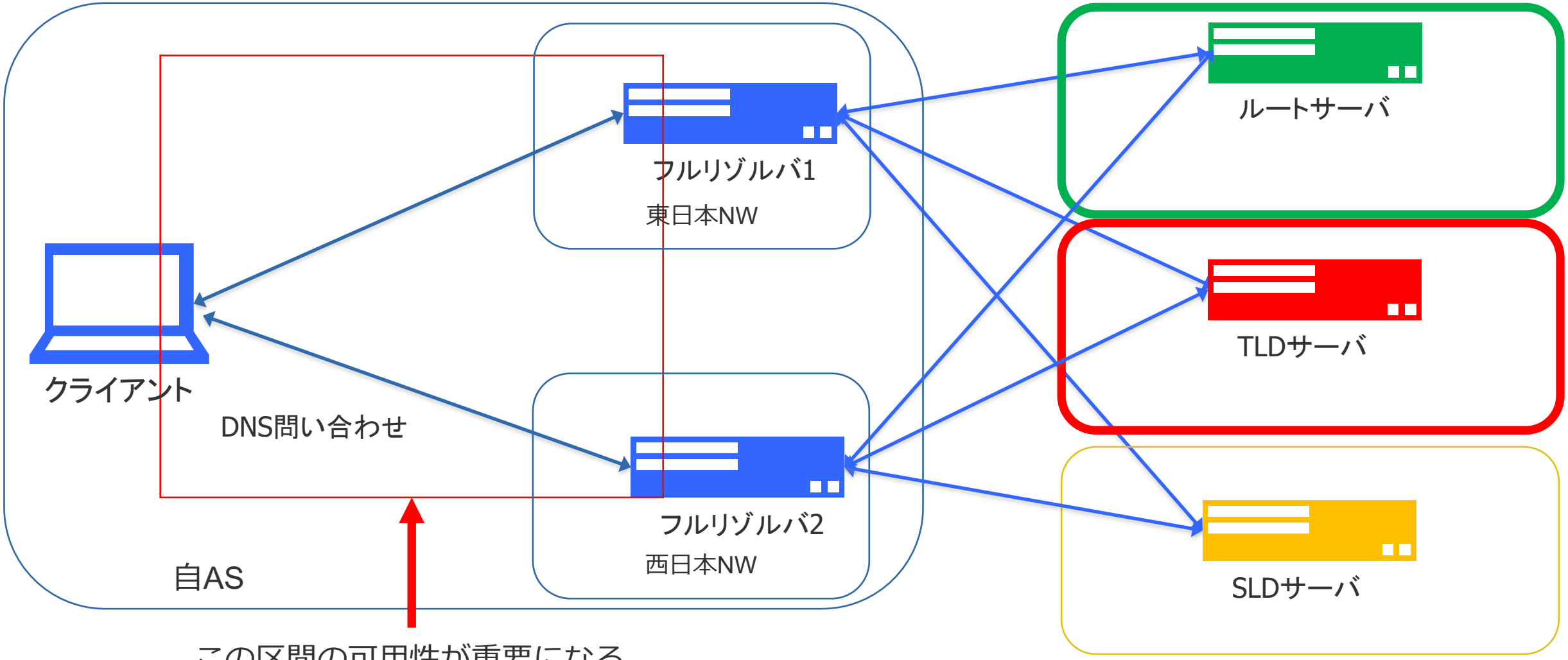
フルサービスリゾルバとは – 可用性

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



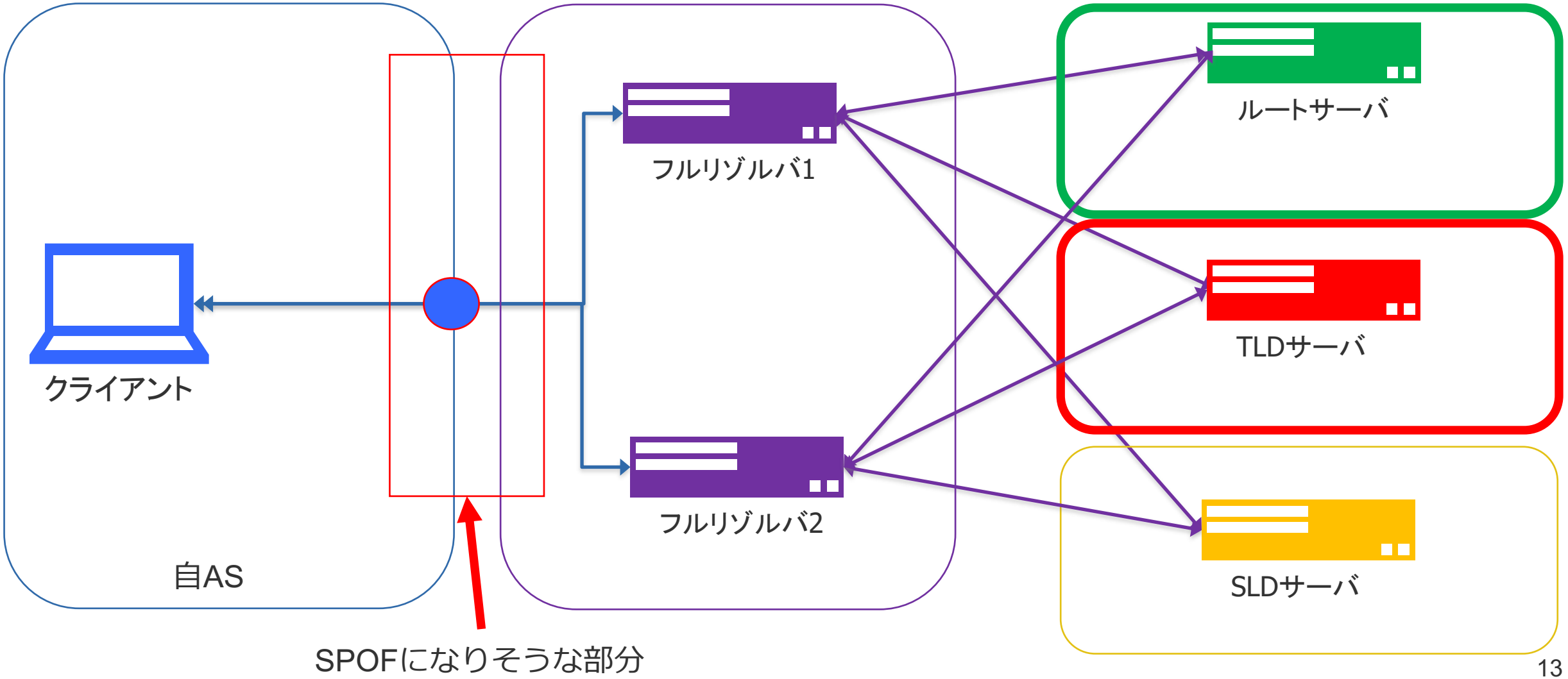
フルサービスリゾルバとは – 可用性

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



フルリゾルバをアウトソースする上での観点

1. 可用性
2. 契約面
3. プライバシー

時間の関係で、今回は可用性にフォーカスします

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

クライアントと、フルリゾルバサービス間の可用性

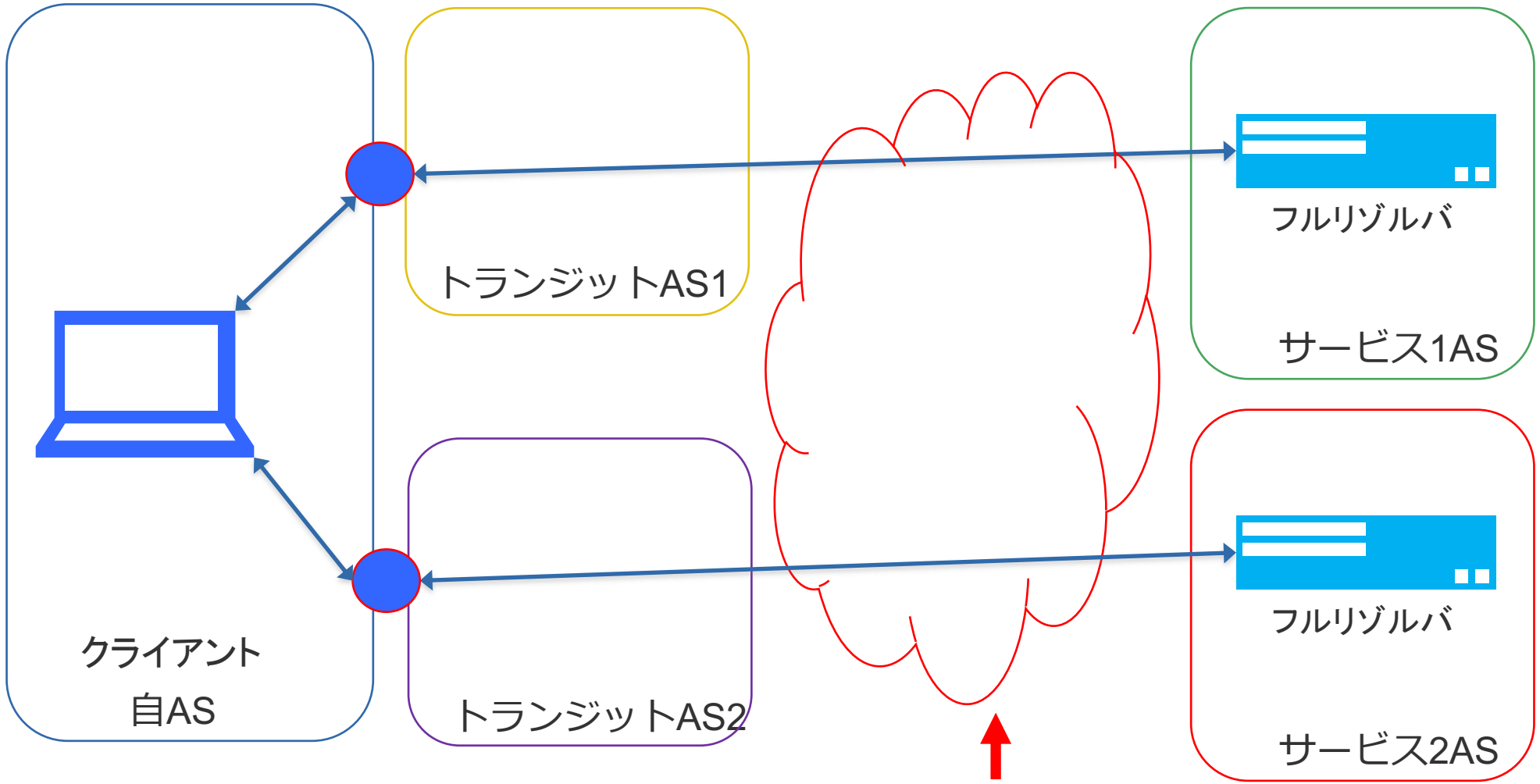
- フルリゾルバサービスとの直接接続ができない限り、可用性は下がる
- 当たり前だが、接続形態で不確実性が上がる
  - Private peer < IX接続 < トランジット経由
  - Private peer以外だと、第３者のトラフィックに巻き込まれる可能性も高い
- 最適な利用形態はどのようなかたちなのか

SPOFを制御することを考える

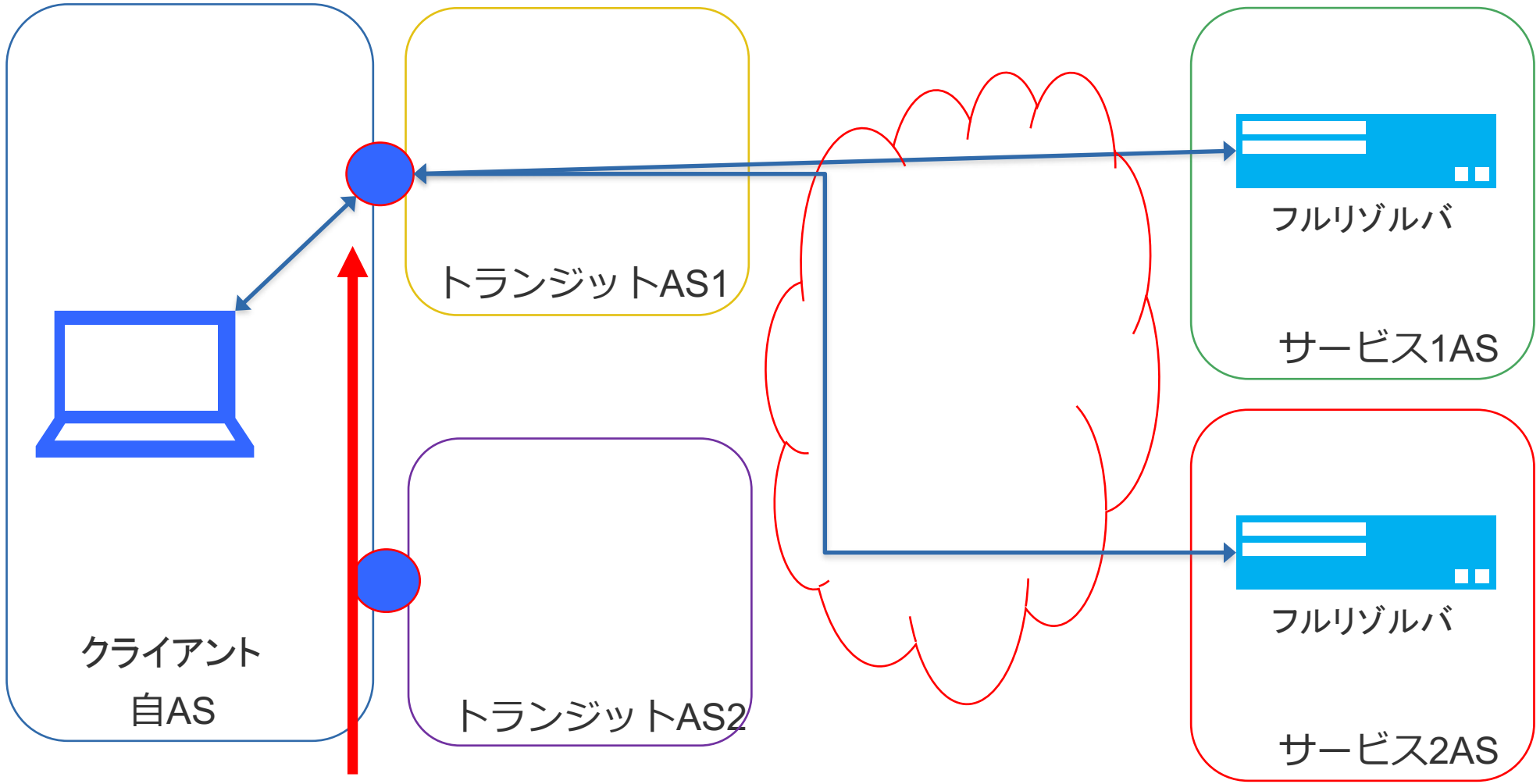
- SPOFがなるべくエッジ付近になるようにトラフィックエンジニアリング
- 接続形態別に考える

注)
この先、Peerって書いてあるのは、直接BGP Peerしている関係という意味です。
Paid Peer, トランジットも含まれます

- PeerしていないASのサービス使うのは難しい
  - トランジット経由だと、経路が変わっていつの間にかSPOFになる可能性も

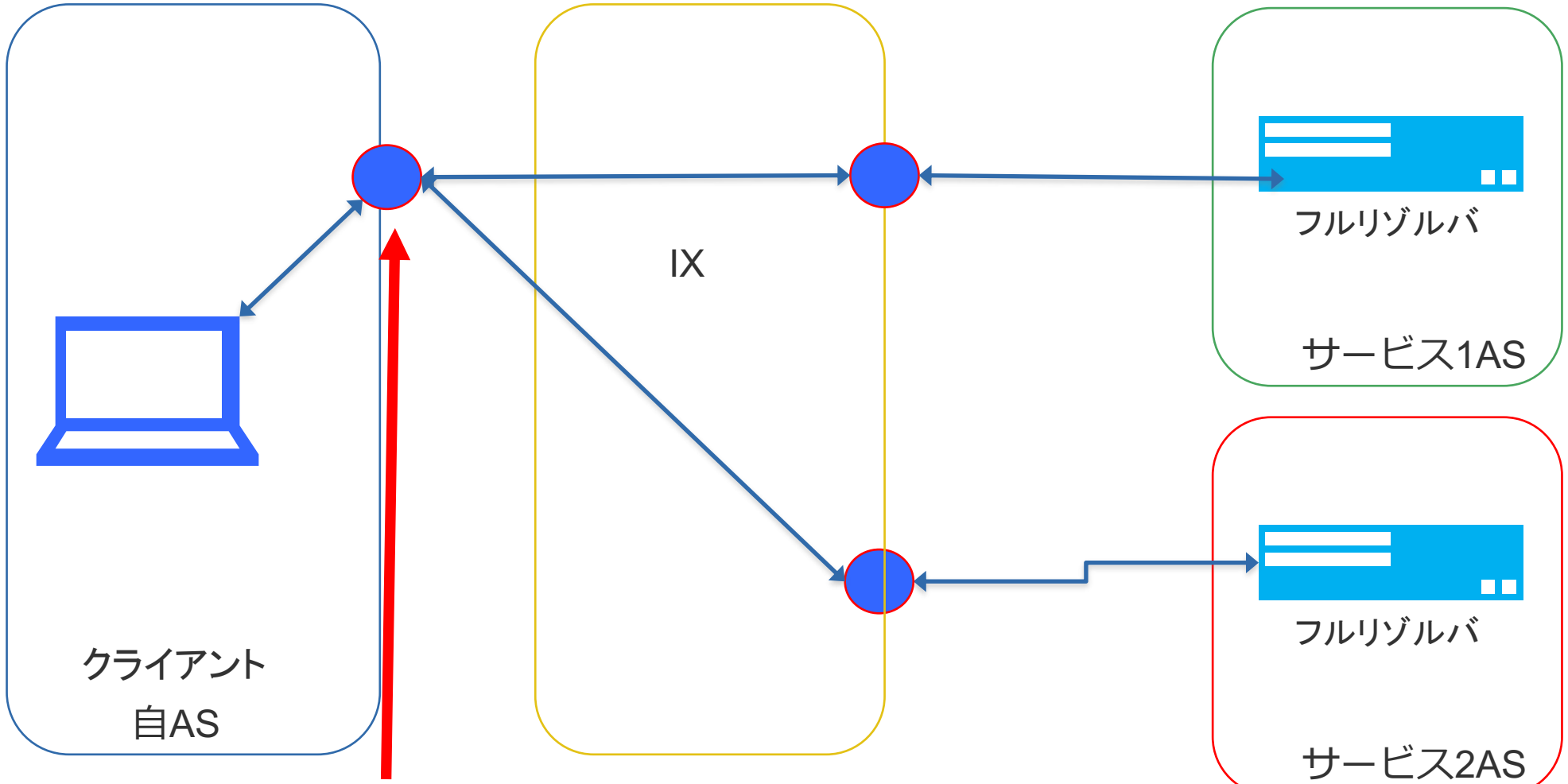


- PeerしていないASのサービス使うのは難しい
  - トランジット経由だと、経路が変わっていつの間にかSPOFになる可能性も



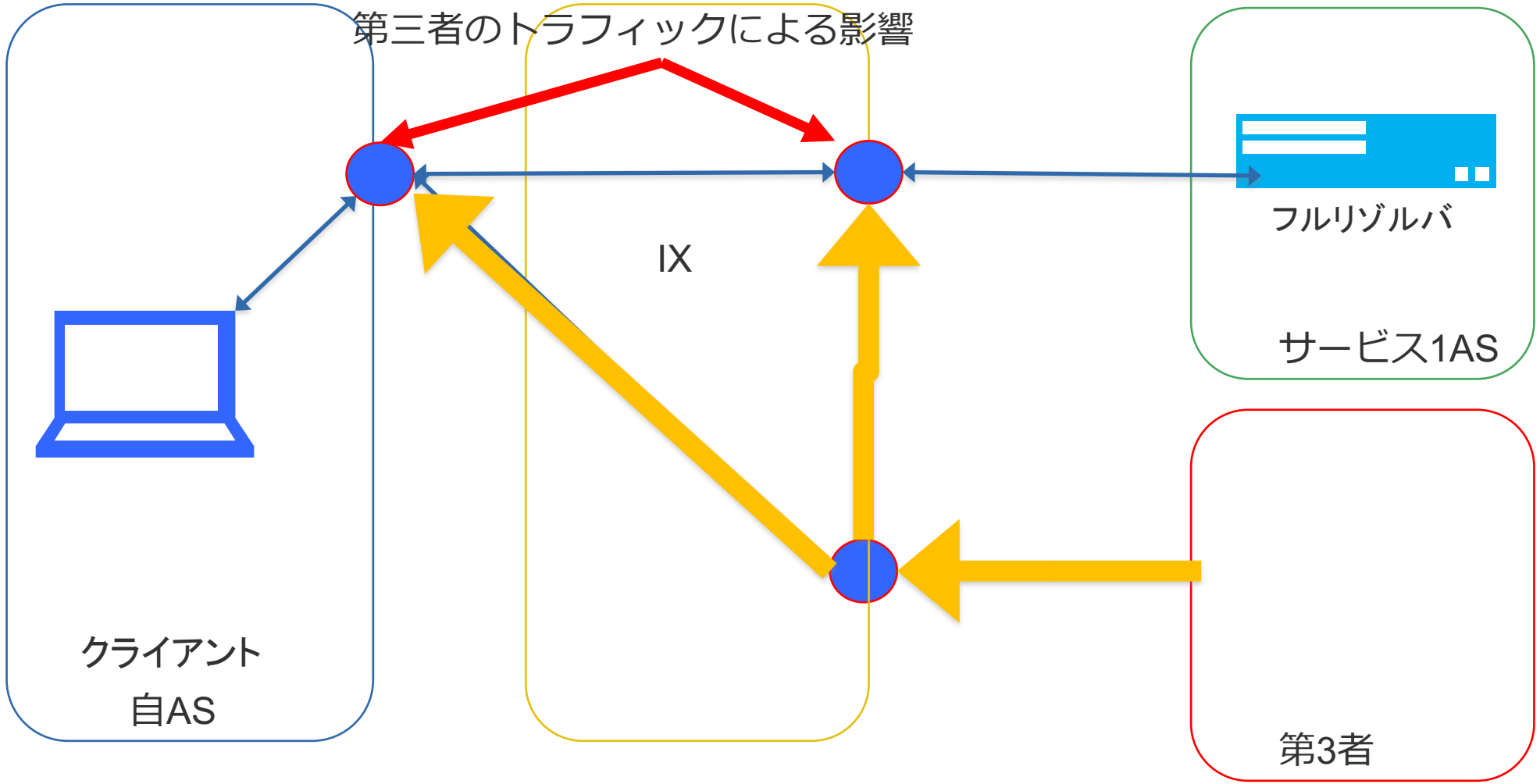
自AS側は何も変更してないが、経路が変わってSPOFができた

- Peerしてたとしても安全とは言い難い
  - IXの場合



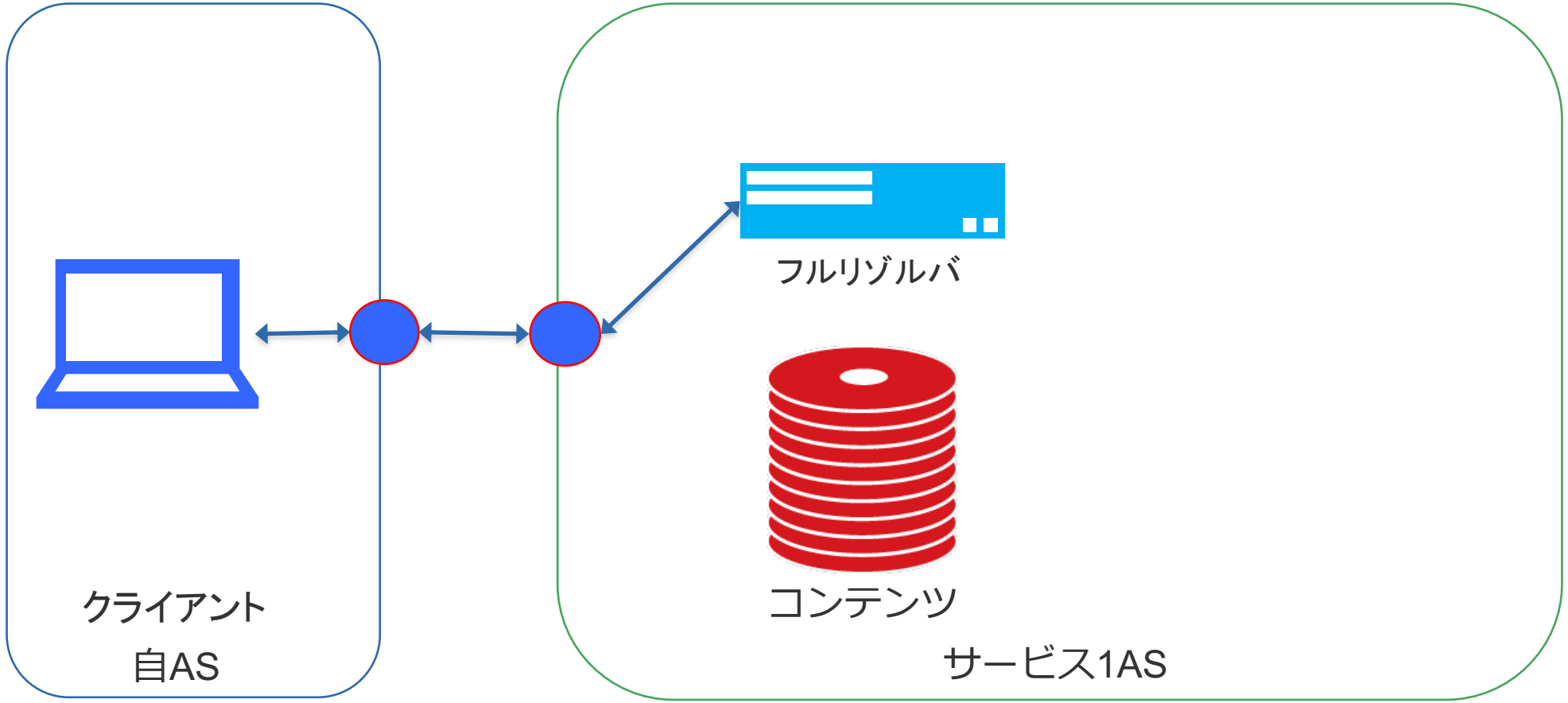
IXの場合、同じポートを通る可能性

- Peerしてたとしても安全とは言い難い
  - IXの場合

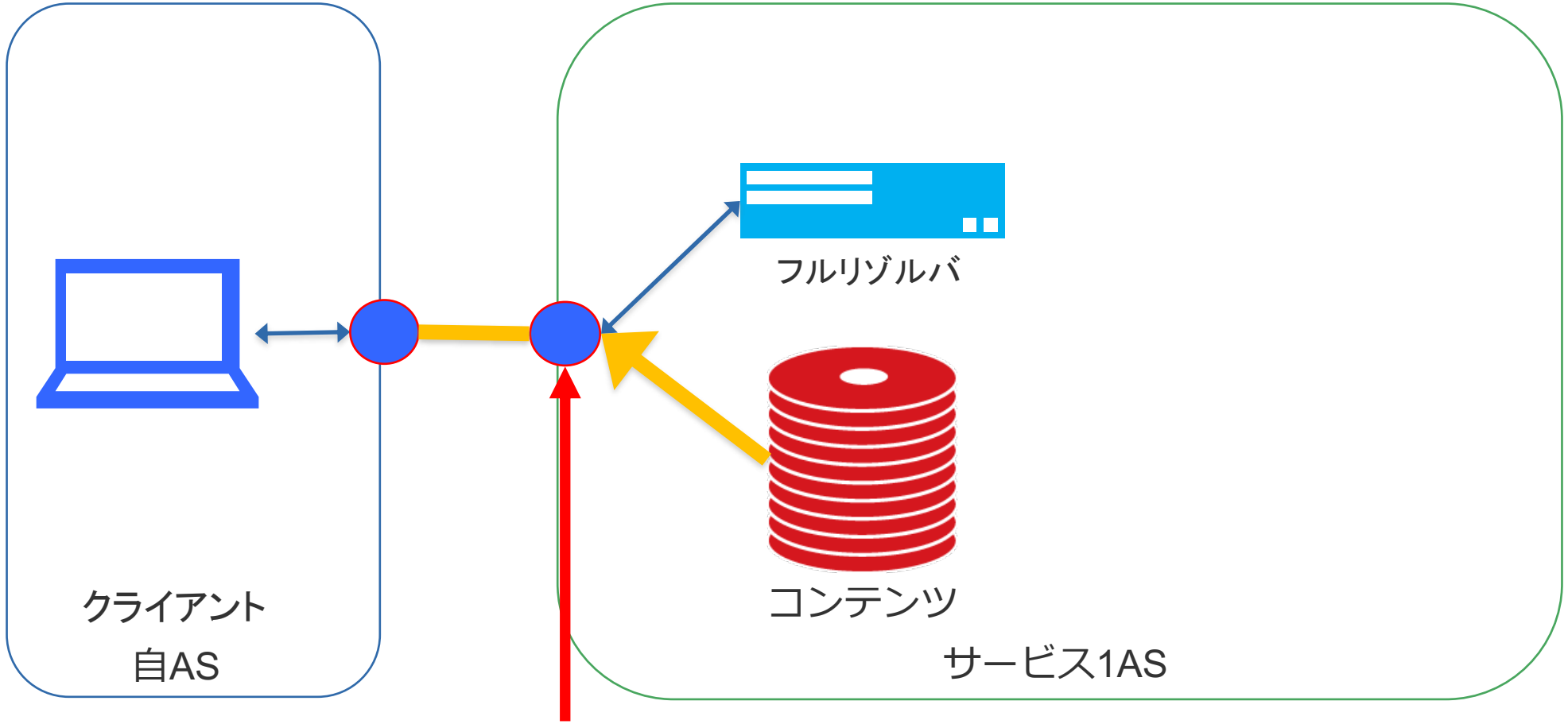


IXを分ける、プライベートピアにするなどの設計が必要

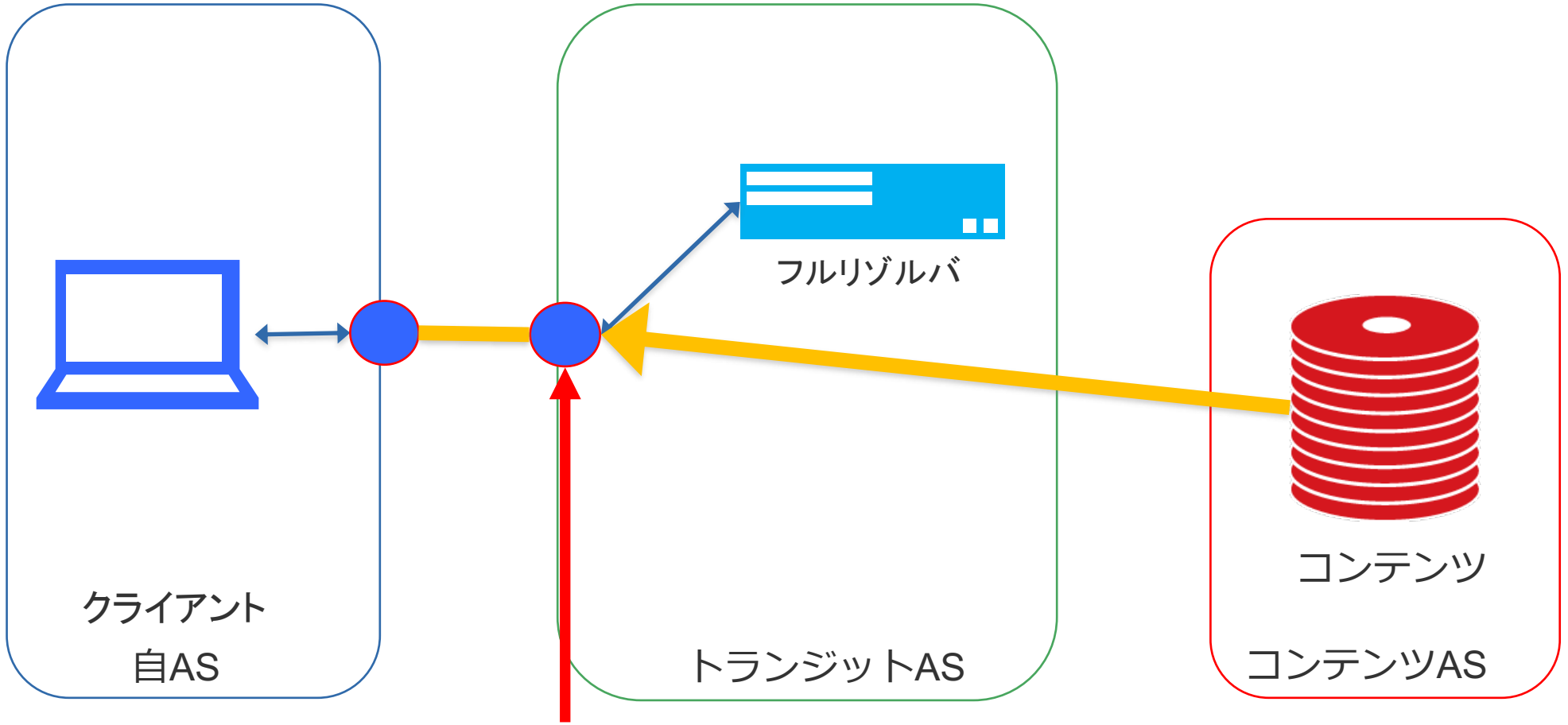
- プライベートピアの場合
  - サービス側がコンテンツを持っている場合は、バーストトラフィックで埋まる可能性がある。



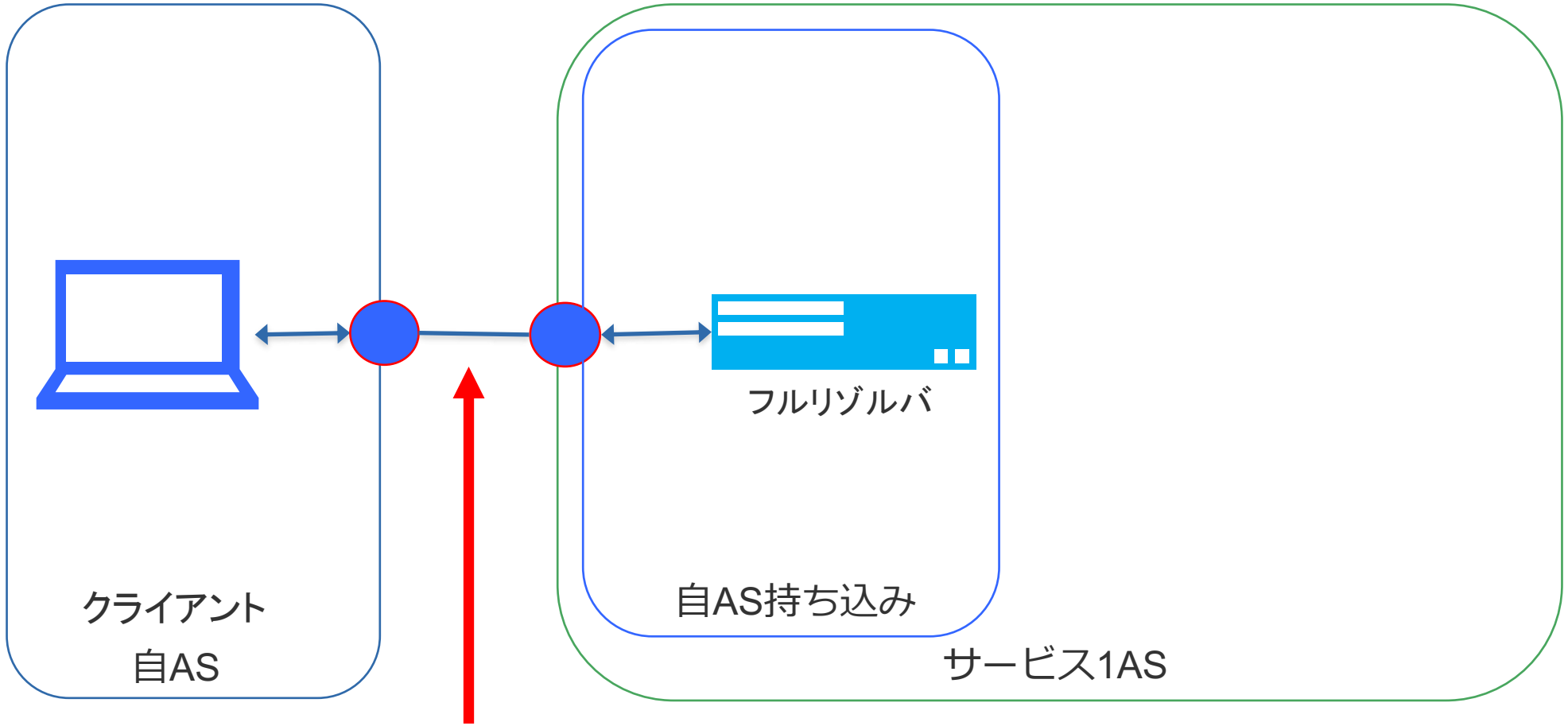
- プライベートピアの場合
  - サービス側がコンテンツを持っている場合は、バーストトラフィックで埋まる可能性がある。



- サービス側が、トランジットASだった場合も同じ現象が起こり得る
  - NOEXPORTすればいいんだろうけど。。



- 直接接続の場合
  - サービス専用の回線が引けるのが一番望ましい
  - これだと、自前とほぼ同等の可用性が望める

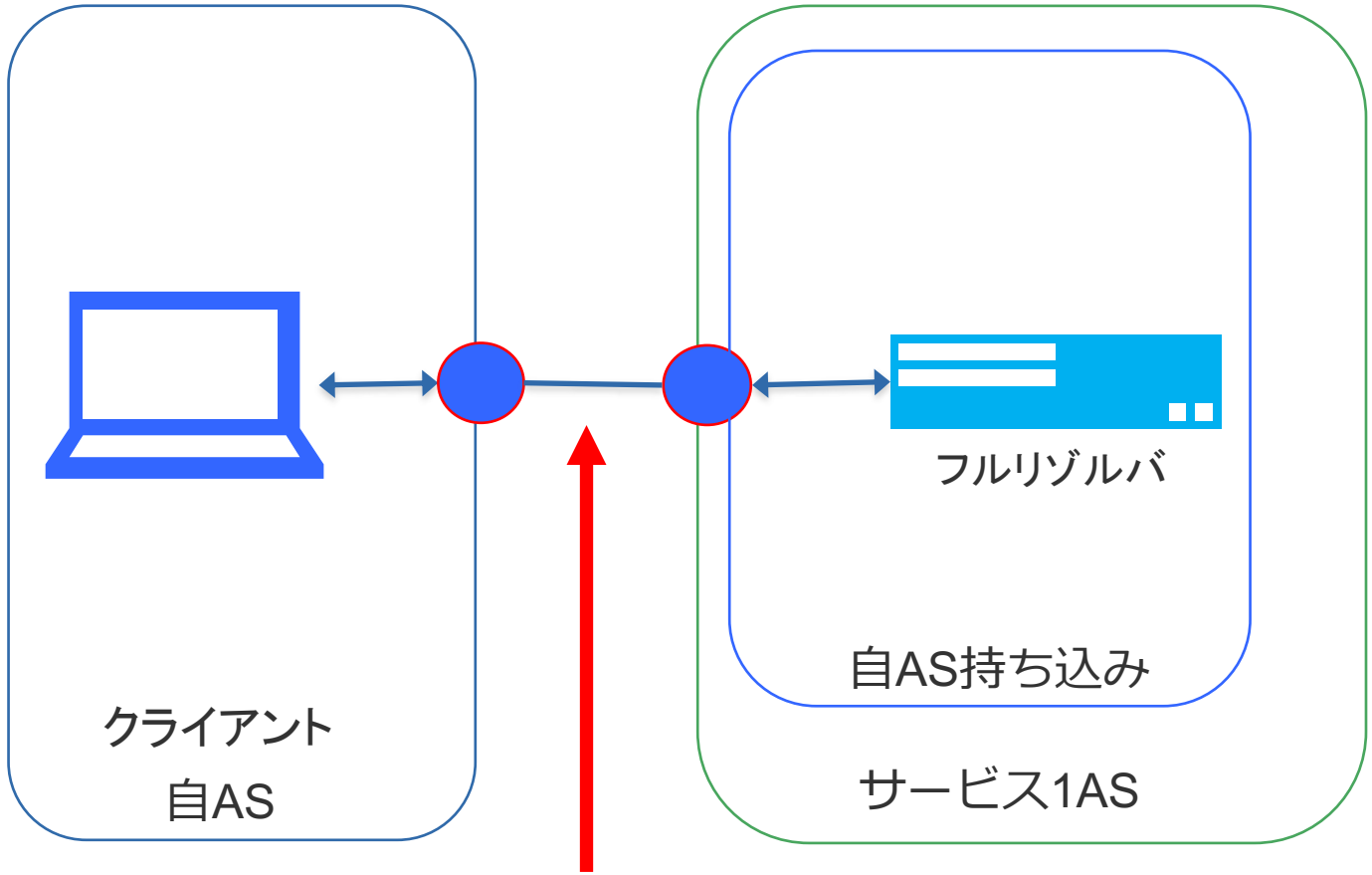


それぞれの利用パターンでの接続形態

- 全てのフルリゾルバの系を同じ外部サービスに出す場合
- 全てのフルリゾルバの系をそれぞれ、別の外部サービスに出す場合
- 一部のフルリゾルバの系を外部サービスに出す場合

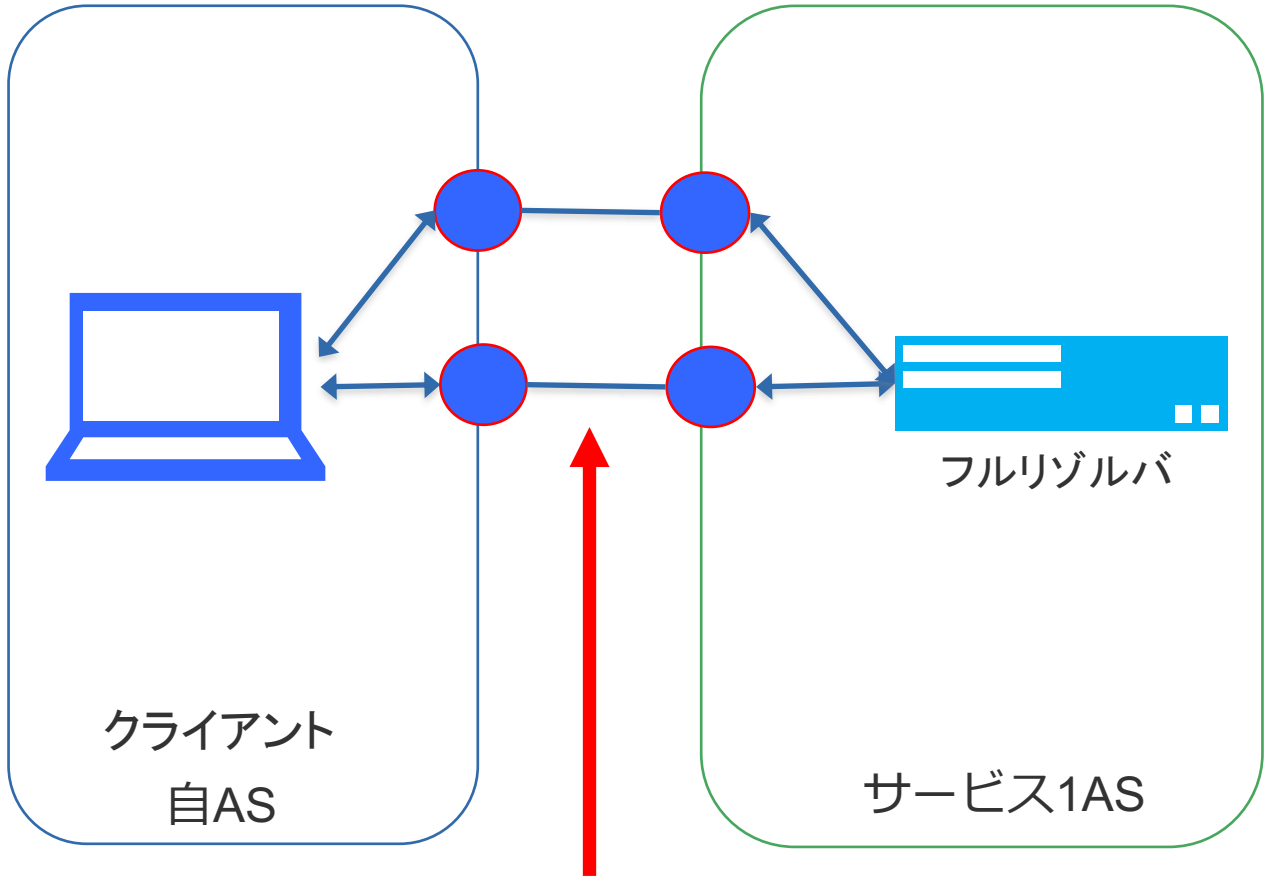
全てのフルリゾルバの系を同じ外部サービスに出す場合

- 系が落ちることは許容できない
- 基本的にこの構成はお勧めできない
- 利用する場合はフルリゾルバサービスと直接接続できるようなサービスを使う



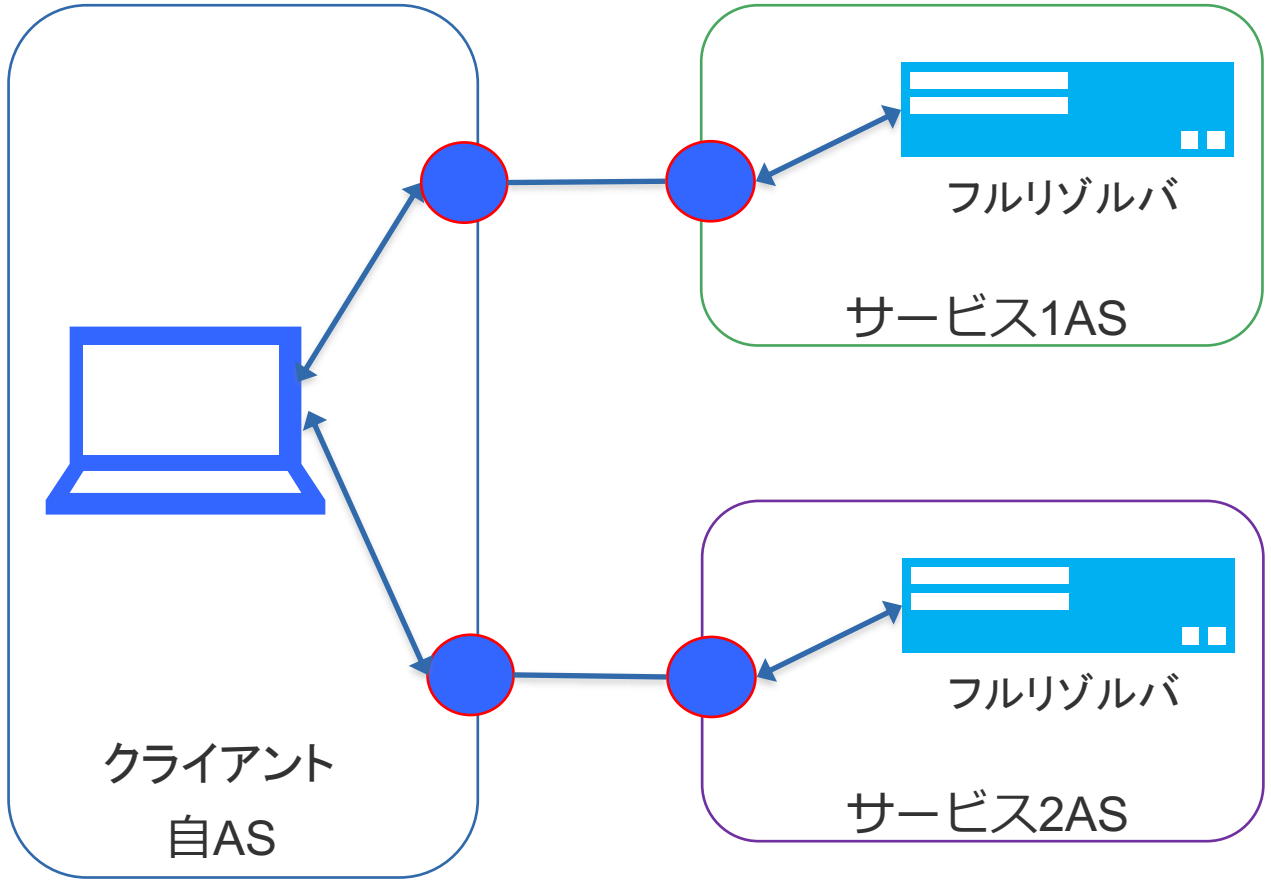
全てのフルリゾルバの系を同じ外部サービスに出す場合

- 系が落ちることは許容できない
- 利用する場合はフルリゾルバサービスと直接接続できるようなサービスを使う
  - できれば他拠点で接続するのが望ましい



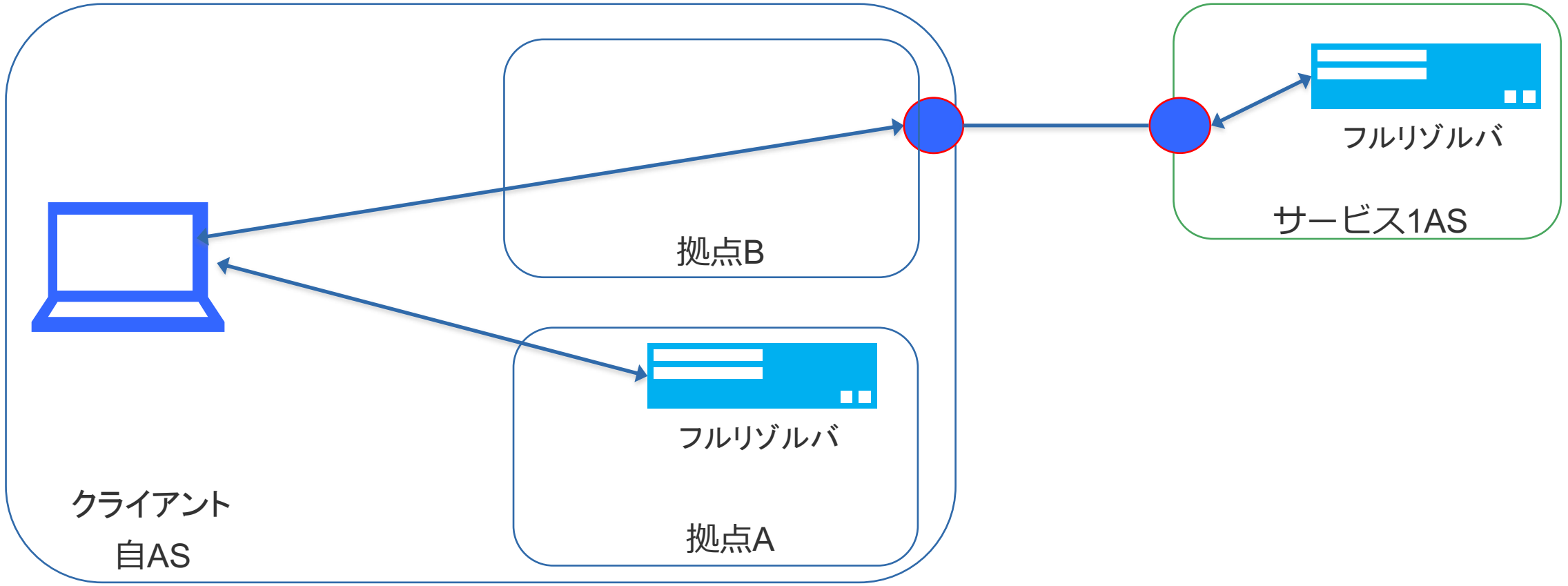
全てのフルリゾルバの系をそれぞれ、別の外部サービスに出す場合

- どちらかの系が障害で止まるのは許容する
- 両サービスが、異なる拠点、機器に収容されていること
  - これを担保するために、両サービスとピアを行う



一部のフルリゾルバの系を外部サービスに出す場合

- どちらかの系が障害で止まるのは許容する
- ISP内部のフルリゾルバ系と異なる拠点、機器に収容されていること
    - これを担保するために、ピアを行う



1. 可用性
2. 契約面
3. プライバシー

ISPとしてフルリゾルバの提供をやめてしまう場合

- 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、どうやって同意をとるのか

- 契約時に同意を取る
  - 一番確実で、明確に同意が取れる
- 既存契約
  - オプトイン方式
    - 同意を取った契約者から、リゾルバを変更する
    - 利用時に明確に同意がとれている
    - 既存契約者全体に同意を取るのが大変
  - オプトアウト方式
    - 同意しない場合は、エンドユーザにオプトアウト用のフルリゾルバに変更してもらう
    - 告知後一定期間後に、DHCP等で配るフルリゾルバを変更する
    - 悪性ドメイン名のフィルタリングとかの同意で使われる手法
    - 明確に同意が取れているわけではない
      - 適用できるかは精査が必要
      - 私見ではPublic DNSサービスとエンドユーザの契約になるので、第三者のISPが勝手に利用させる、この手法は取れない
  - オプトイン、オプトアウトでも、ISP運用のDNSサーバが残る
- 完全新規のサービスで無い限り、Public DNSを直接ユーザに配るのは非現実的

1. 可用性
2. 契約面
3. プライバシー

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、プライバシーポリシーがフルリゾルバサービスに必要か

RFC8932 「Recommendations for DNS Privacy Service Operators」6.1.1 Policy

- IPアドレスは個人識別情報として扱うことを定めること
- データの収集と共有
  - IPアドレスが含まれているか
  - パートナー、第3者への共有
  - データが集約されるか、仮名化、匿名化できるか
  - etc…

- この辺りが明記されていることは必須
- 生のIPアドレスを長期保存するところは、アウトソース先としては選定しずらい
  - 一つの指標として、MozillaがFirefox向けのDoHプロバイダーに求めている
    保存期間は24時間まで
- 生のIPアドレスのデータの第三者への提供など、正当業務行為の範疇を超えた通信の秘密の侵害
  顧客の明確な同意があれば大丈夫だが、オプトアウトレベルの同意だとNGか。

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、Maskしている
  - 大きすぎると、割り当てCIDRを超えてしまう可能性
    - 海外判定されたりする
  - 細かすぎると、プライバシー面への悪影響
  - IPv4だと最小割り当てサイズの/22 ?, IPv6だと/32とか ?
  - そもそもユーザ側で設定できない場合がほとんど

議論タイム

**ISP内で動いているサービスをアウトソースする際に、
接続性をどれくらい気にして選定しました？**

**例：
フルサービスリゾルバ
メールサービス
認証系(Radis, LDAP)
最近だと、ROAキャッシュサーバとか**