

ISPの運用経験からのIPv6トラブルシューティング

ソネット株式会社
ネットワーク基盤事業部門

上根義昭

本プレゼンテーションについて

- インターネット接続サービスを提供するにあたり、IPv6ネットワークを運用する際に発生しうる一般的なトラブル事例についてその原因やトラブルシューティングを解説します(70分)。

略歴

- 2001年4月ソネット株式会社(旧ソニーコミュニケーションネットワーク)入社
 - フレッツサービス設計/構築/運用
 - バックボーン・データセンタ設計/構築/運用
 - NURO光設計/構築

- その他
 - IPv6普及・高度化推進協議会
 - IPv4/IPv6共存WGにてガイドライン作成に参加

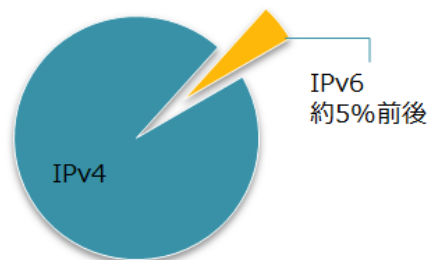
はじめに

So-net : IPv6対応状況

対象		対応状況	備考
バックボーン	対外接続	対応済み	•Transit/Peer/IXについて可能な限りDual接続実施
	コアネットワーク		•機器間、拠点間は全てDual接続実施
サービス	メール		•POP/SMTP共に対応済み
	Web		
	DNS		
接続サービス	コミュファ光		•2013年9月より提供中
	auひかり		
	NURO光		•NURO光利用全ユーザーにIPv6提供中
	フレッツ光 (PPPoE)		<ul style="list-style-type: none"> •2014年上期よりHGW対応開始 •愛知を除く全エリアの「フレッツ光ネクストコース」が対象 •残る愛知エリアについても2015年7月対応完了予定

So-net「フレッツ光ネクストコース」におけるIPv6利用状況

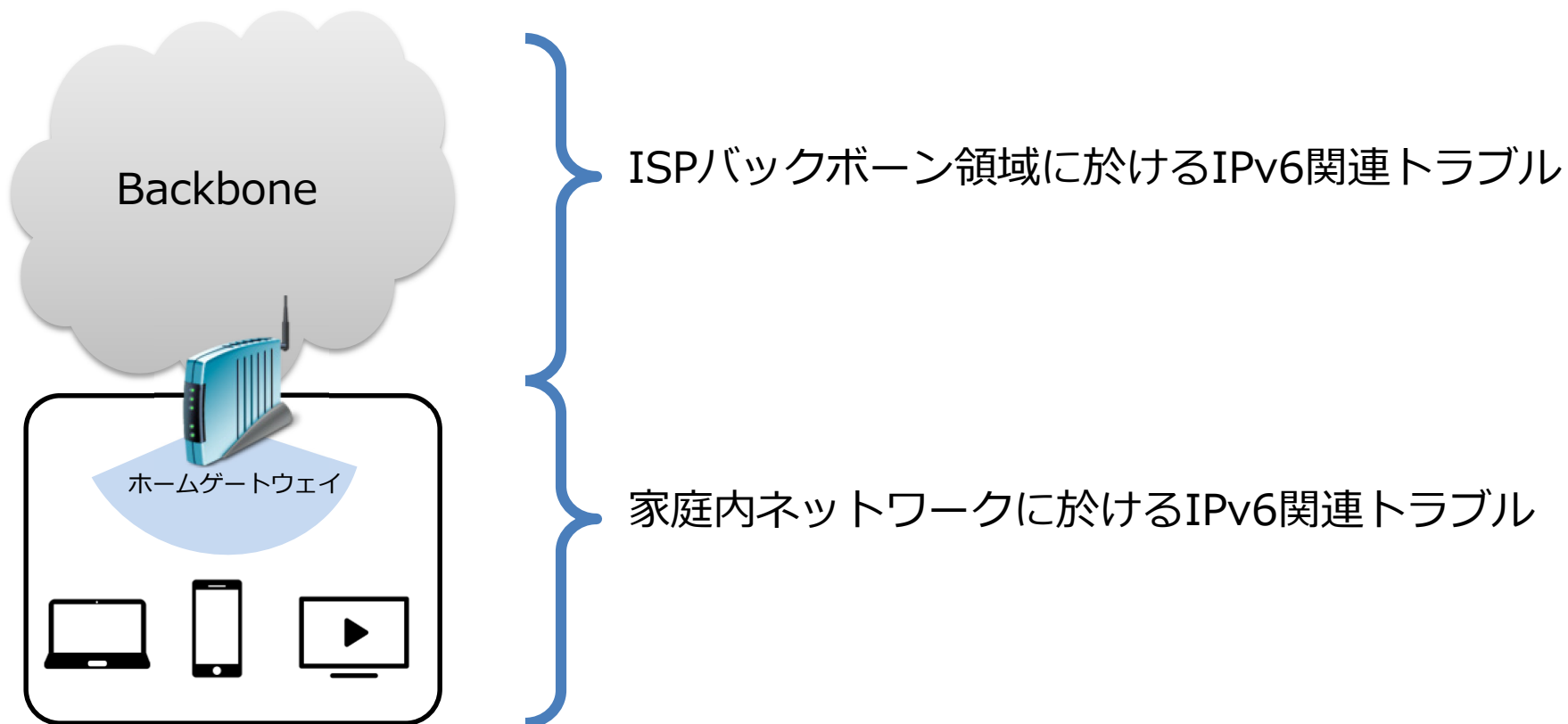
- IPv4/IPv6トラフィック比率



- IPv6利用ユーザー数(Session数)推移



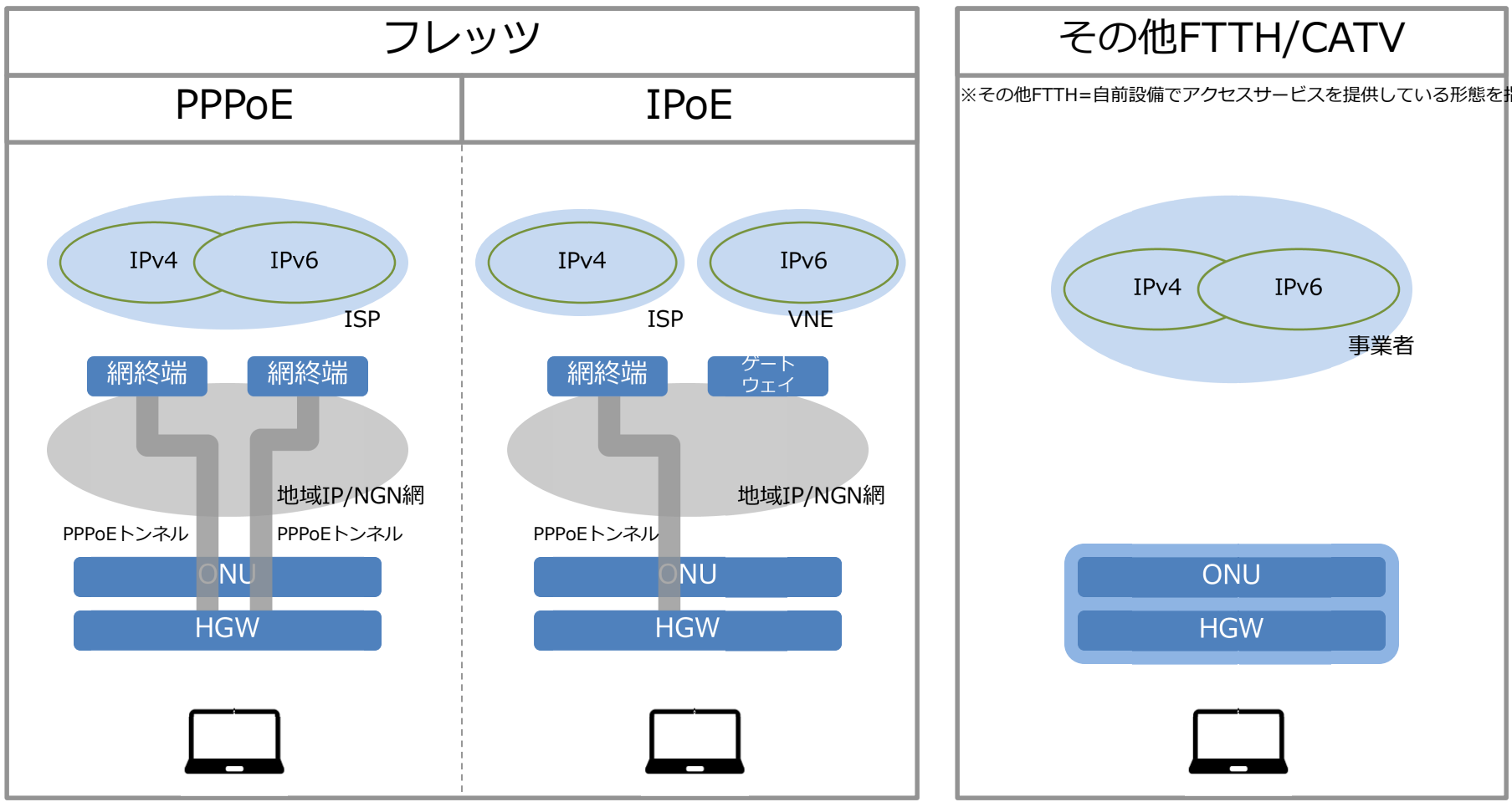
0. 説明の範囲と目次



目次

- ✓ IPv4/IPv6トロポジ違いによる注意点
- ✓ ホームゲートウェイによるサーバ負荷増大事象
- ✓ 家庭内ネットワークでの通信不可事例
- ✓ バックボーンでのPath MTU Discovery問題事例
- ✓ バックボーンでのトラブル事前対策
- ✓ まとめ

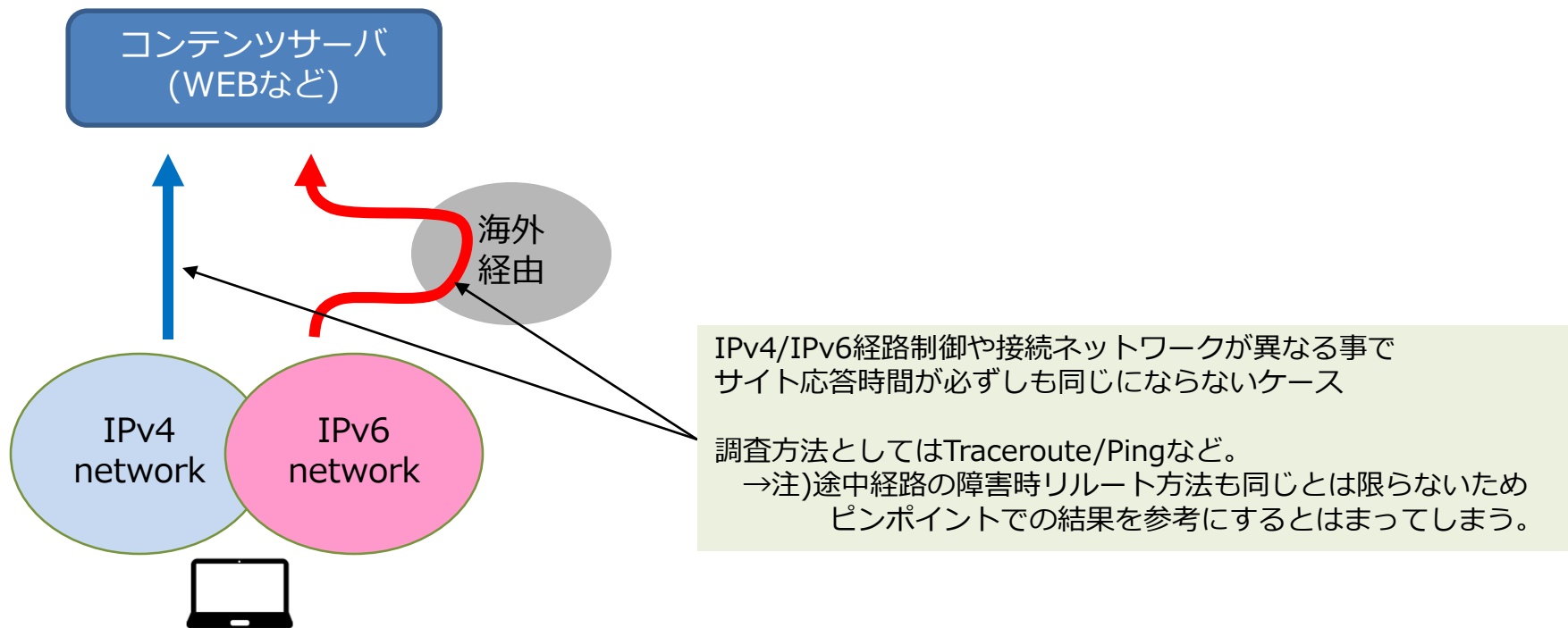
0. IPv4/IPv6 トロポジ違いによる注意点



0. IPv4/IPv6 トロポジ違いによる注意点

- IPv4/IPv6で運用ポリシーが違うケース

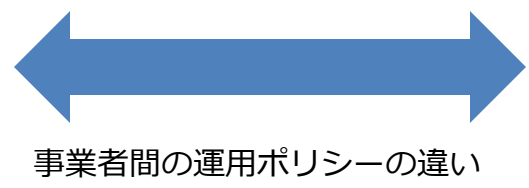
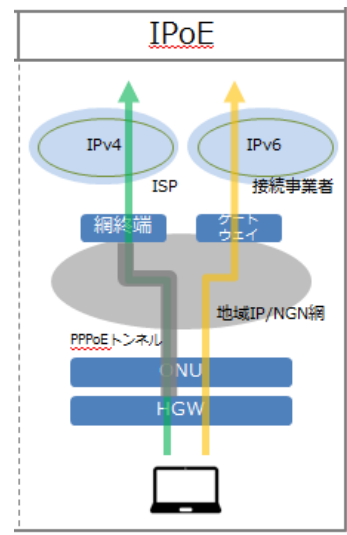
– IPv4とIPv6でネットワーク構成が異なる場合



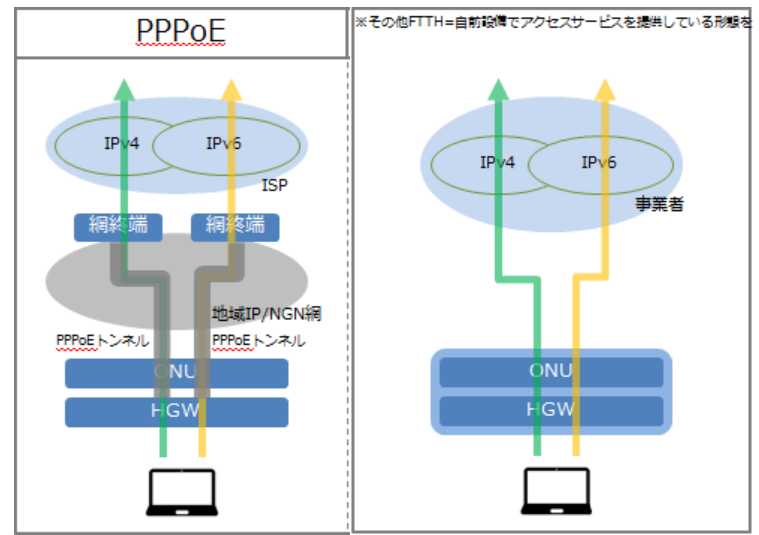
0. IPv4/IPv6 トロポジ違いによる注意点

- IPv4/IPv6で運用ポリシーが違うケース
 - IPv4とIPv6で提供事業者が異なる場合

提供事業者が異なる



提供事業者が同じ



目次

- ✓ IPv4/IPv6トロポジ違いによる注意点
- ✓ **ホームゲートウェイによるサーバ負荷増大事象**
- ✓ 家庭内ネットワークでの通信不可事例
- ✓ バックボーンでのPath MTU Discovery問題事例
- ✓ バックボーンでのトラブル事前対策
- ✓ まとめ

1.1 ホームゲートウェイによるサーバ負荷増大事象

- DNSでの負荷を観測していると、ある日突然負荷状態が上昇してしまった・・・！



1.1 ホームゲートウェイによるサーバ負荷増大現象

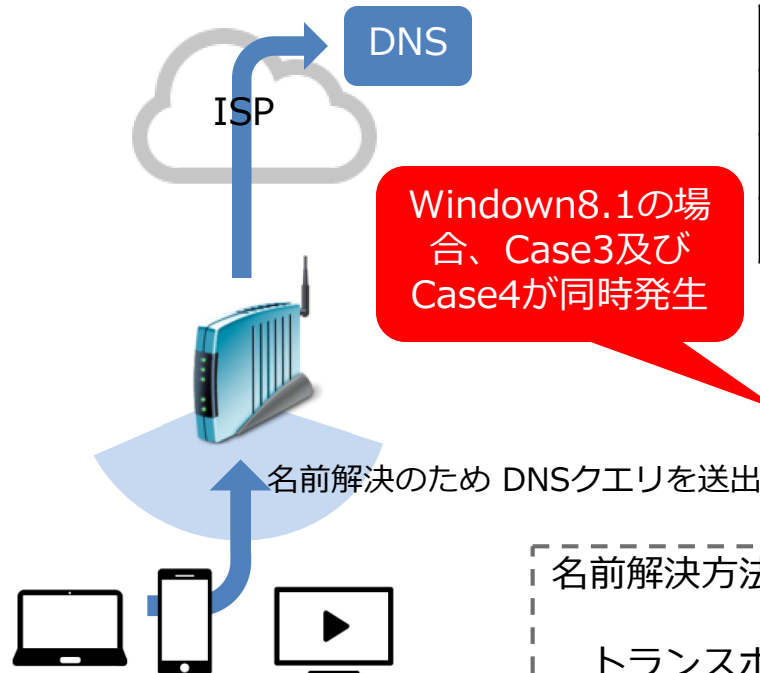
【解説】

- DNS(Domain Name System)とは？
 - 端末が名前解決を行う際にドメイン名をIPアドレスに変換する仕組み
 - 例1 Aレコード(IPv4アドレス)
 - » www.so-net.ne.jp → 192.0.2.80
 - 例2 AAAAレコード(IPv6アドレス形式)を要求
 - » www.so-net.ne.jp → 2001:db8:AAAA:AAAA::80
- DNSサーバへの問い合わせ方法（トランスポート）
 - IPv4 DNSへIPv4パケットで問い合わせ
 - » 192.0.2.53
 - IPv6 DNSへIPv6パケットで問い合わせ
 - » 2001:db8:AAAA:AAAA::53

★同じドメイン名でもA(IPv4)/AAAA(IPv6)両方のレコードを持つ場合があります。

1.1 ホームゲートウェイによるサーバ負荷増大事象

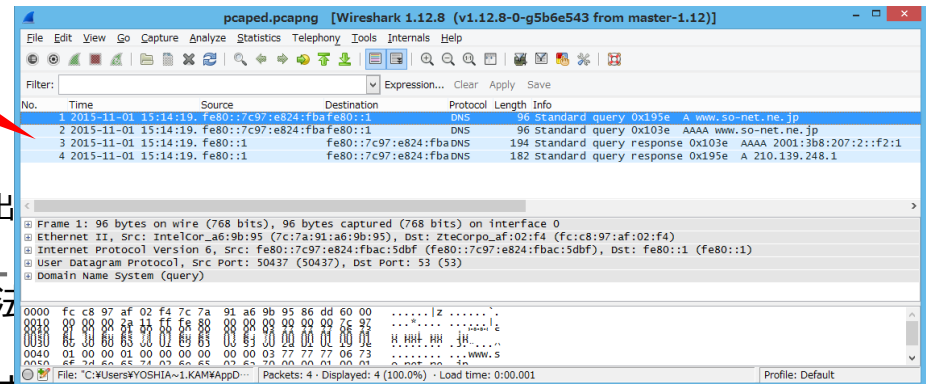
- IPv4 / IPv6デュアル環境における名前解決パターン



DNSクエリ送パターン

case1	IPv4トランスポート	+	A
case2	IPv4トランスポート	+	AAAA
case3	IPv6トランスポート	+	A
case4	IPv6トランスポート	+	AAAA

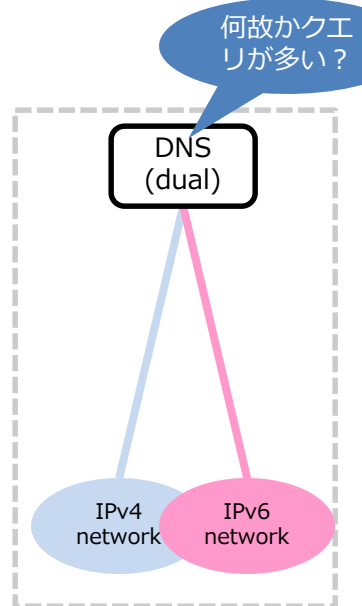
名前解決方法
トランスポート IPv4 or IPv6 ?
クエリ A or AAAA ?



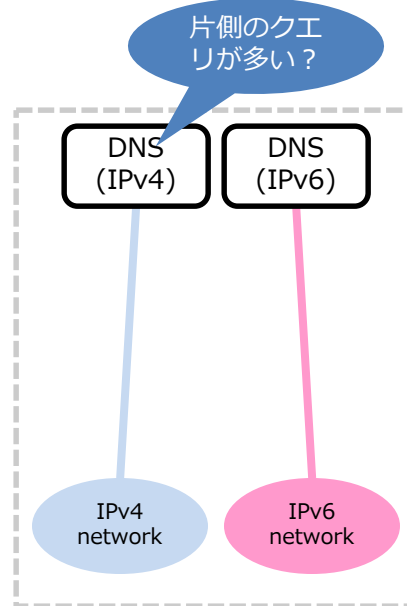
1.1 ホームゲートウェイによるサーバ負荷増大現象

- 今回の場合、実際にはどのように見えるのか？

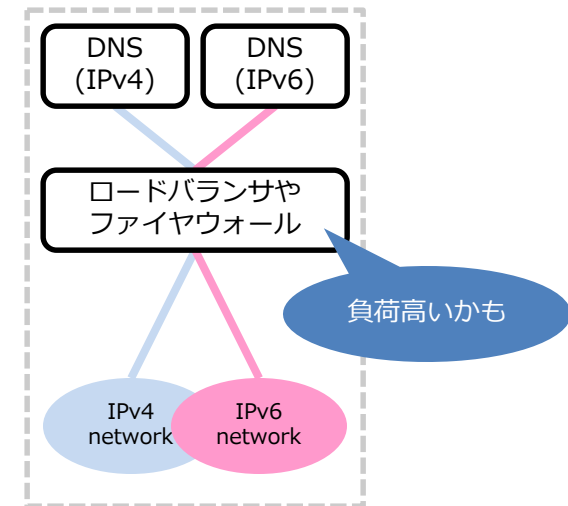
– ケースによりそれぞれの見え方



IPv4/IPv6デュアルスタック収容したサーバポイント



IPv4とIPv6それぞれで収容した各サーバポイント



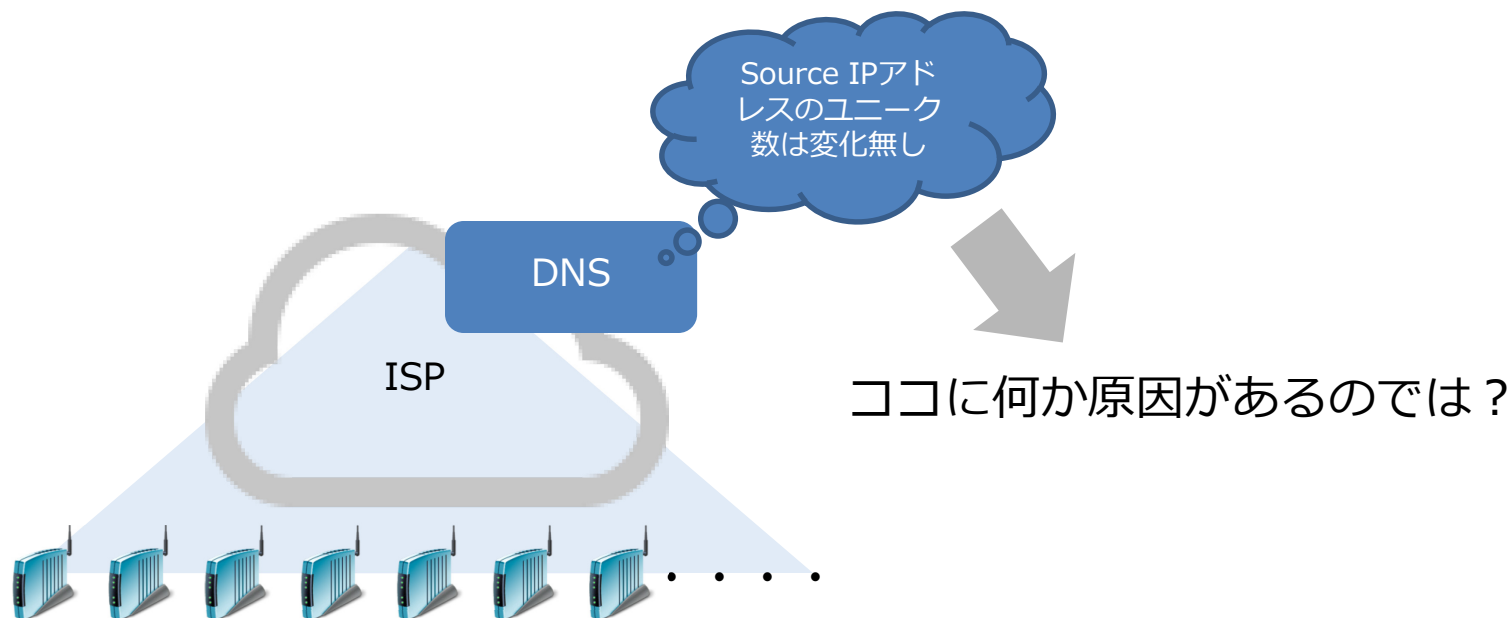
DNS前段に設置した集約ポイント

1.1 ホームゲートウェイによるサーバ負荷増大事象

- 攻撃によるものでしょうか？
 - そもそも適切なDNSクエリでしょうか？
- ISP DNSサーバへの問い合わせとして不適切な逆引き。
 - AAAAレコード正引きとしてホームゲートウェイがお漏らし？
 - 例：Link Local Address fe80::1 (LAN内デフォルトゲートウェイ)
 - 例：Multicast Address ff02::1:3 (LAN内の近隣DNS検索)
- 自社ネットワーク“外”からのDNSクエリ受信が増えてませんか？
 - BCP140 : <https://tools.ietf.org/html/bcp140>
 - DNSサーバが自身のネットワーク“外”から利用され、DNSリフレクタ攻撃の踏み台となってしまう事を防ぐ

1.1 ホームゲートウェイによるサーバ負荷増大事象

- 今回は・・・
- Source IPアドレスのユニーク数の割合に注目！



1.1 ホームゲートウェイによるサーバ負荷増大現象

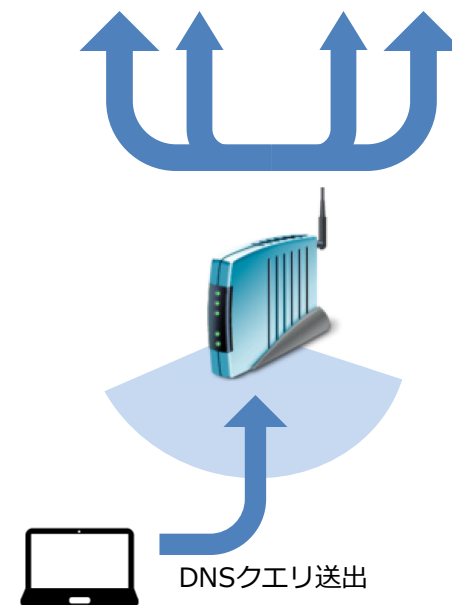
- Source IPアドレスのユニーク数が変わっていないという事は？
- ↓
- 1 端末からの送出クエリ数がそもそも多いのでは？
- あるケース・・・
 - ある特定のホームゲートウェイがメーカーのファームアップデートにより同時送出クエリ数が2x~4xに。

- ★端末からのトランスポートは変更して欲しくない。(MAY)
 - ★Primary/Secondary DNSに対して順番で問い合わせべき。(MUST)
- 出典：『IPv6 家庭用ルータガイドライン第2版』



1. ベンダによる改修対応（要ご相談）
2. 特定サービスに関連する場合、配布DNSレコードの変更（力技!）

A/AAAA, IPv4/IPv6, Primary/Secondary
それぞれのパターンのクエリを同時送出

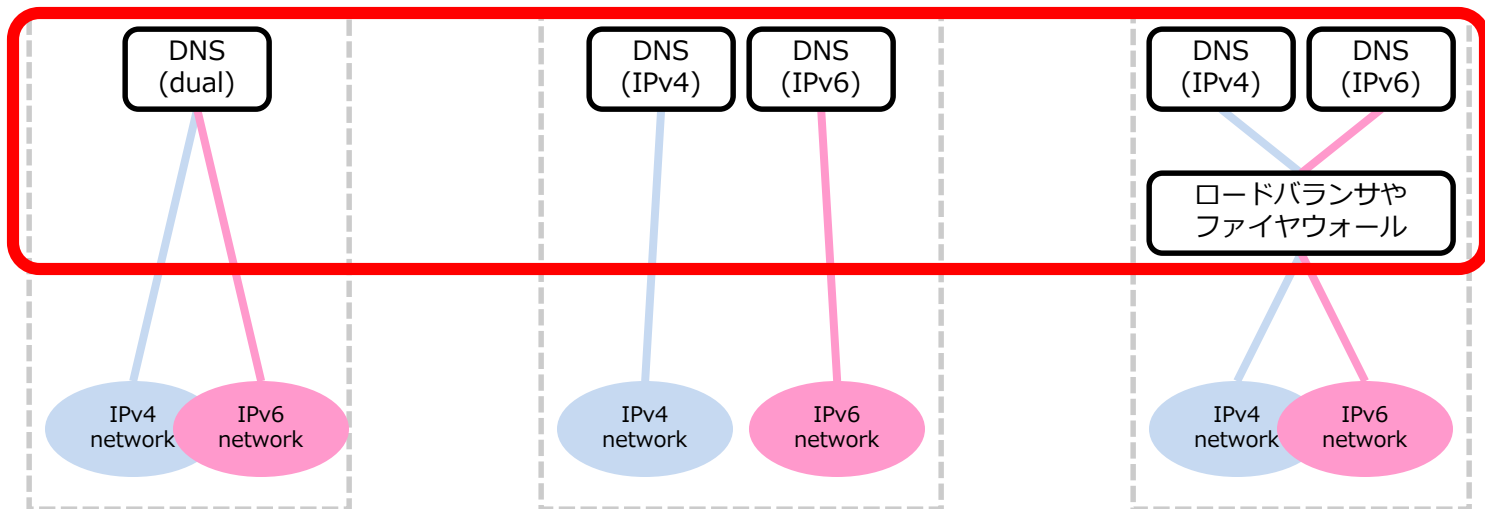


1.1 ホームゲートウェイによるサーバ負荷増大事象

- 予防と対策

- 負荷のモニタ方法の細分化

- →IPv4 / IPv6 更にはA/AAAA別のモニタリングにより早期発見



目次

- ✓ IPv4/IPv6トロポジ違いによる注意点
- ✓ ホームゲートウェイによるサーバ負荷増大事象
- ✓ **家庭内ネットワークでの通信不可事例**
- ✓ バックボーンでのPath MTU Discovery問題事例
- ✓ バックボーンでのトラブル事前対策
- ✓ まとめ

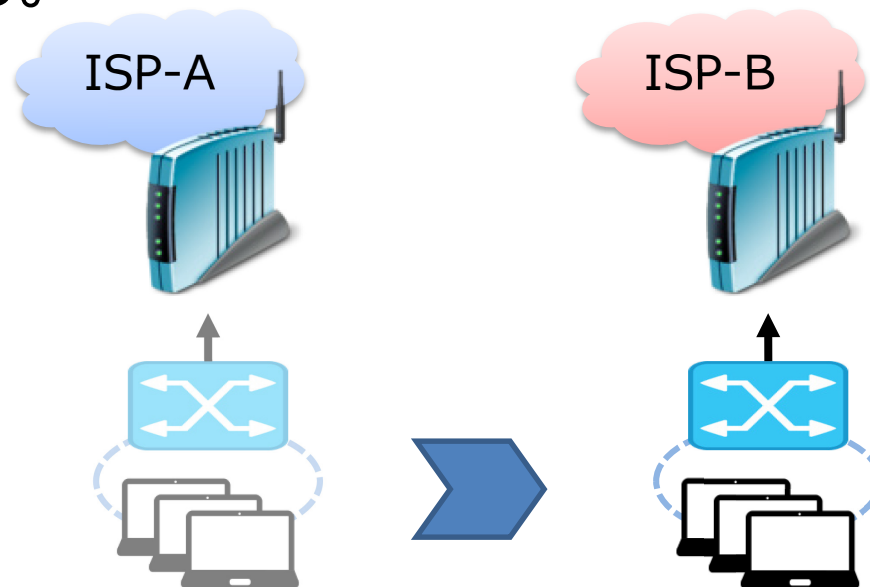
1.2 家庭内ネットワークでの通信不可事例

- 特定の端末で“特定の”IPv6通信が出来ない場合がある。



1.2 家庭内ネットワークでの通信不可事例

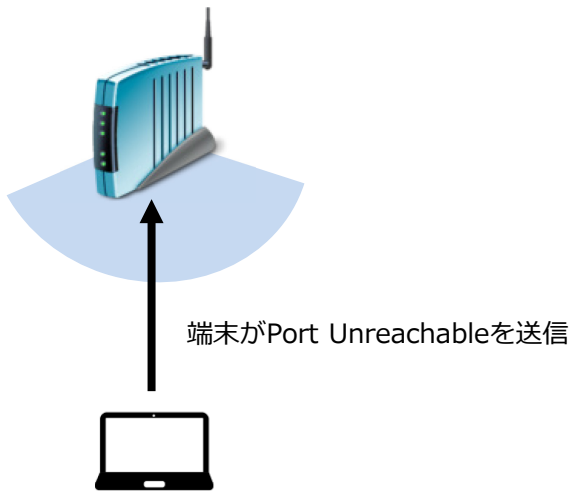
- 端末が利用しているIPは想定したものか？
 - Link断を伴わないセグメント間移動の場合、正しい移動後セグメントのアドレスを利用していない場合も。



L2スイッチごと接続変更を行った場合、
タイミングによって端末側の更新がうまくいかない・間に合わない場合も。

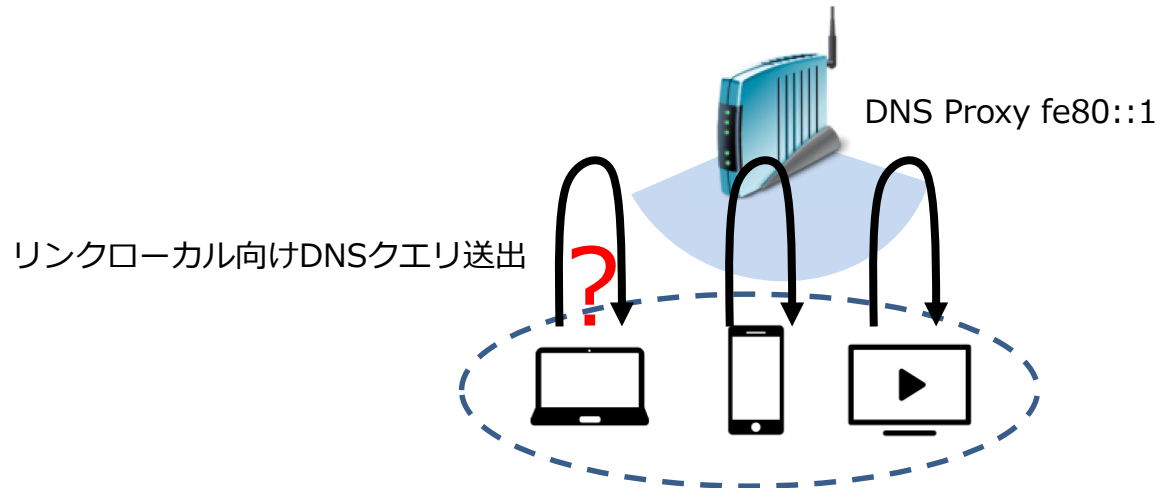
1.2 家庭内ネットワークでの通信不可事例

- 不自然なパケットが“大量に一方方向に”流れていないか？
 - 特定アプリケーションが利用できなかった
 - 調べてみると・・・
 - Port Unreachableが発生しているケース



1.2 家庭内ネットワークでの通信不可事例

- エンドユーザは特にデバッグしにくい
- 「使えない」という申告しか来ない！

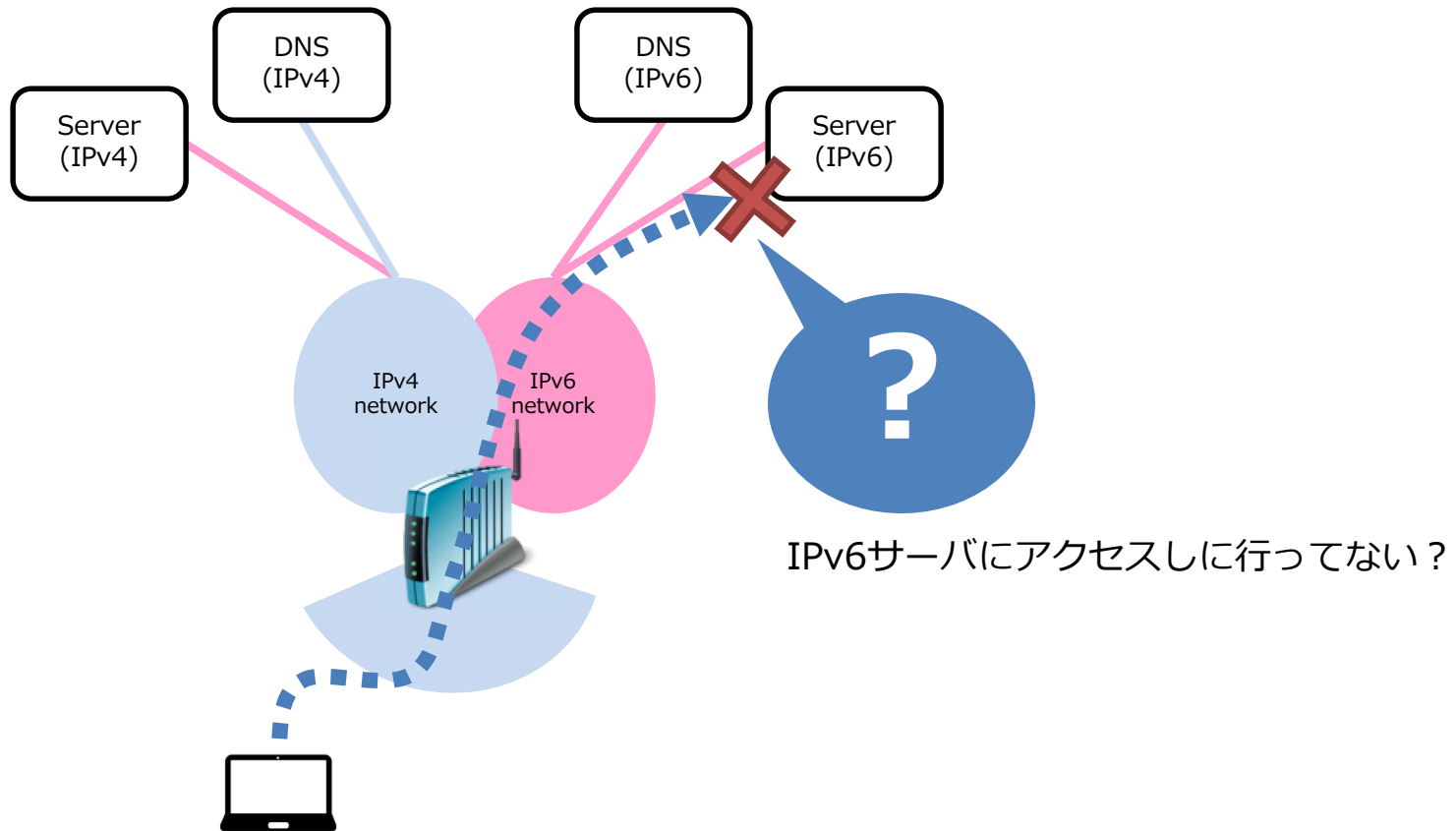


- 特殊パターン例

- Proxy設定しているDNS アドレスがリンクローカルアドレスの場合に、端末は該当アドレスへDNSクエリを送出するが、受け取ってくれない（ポートをとじている）

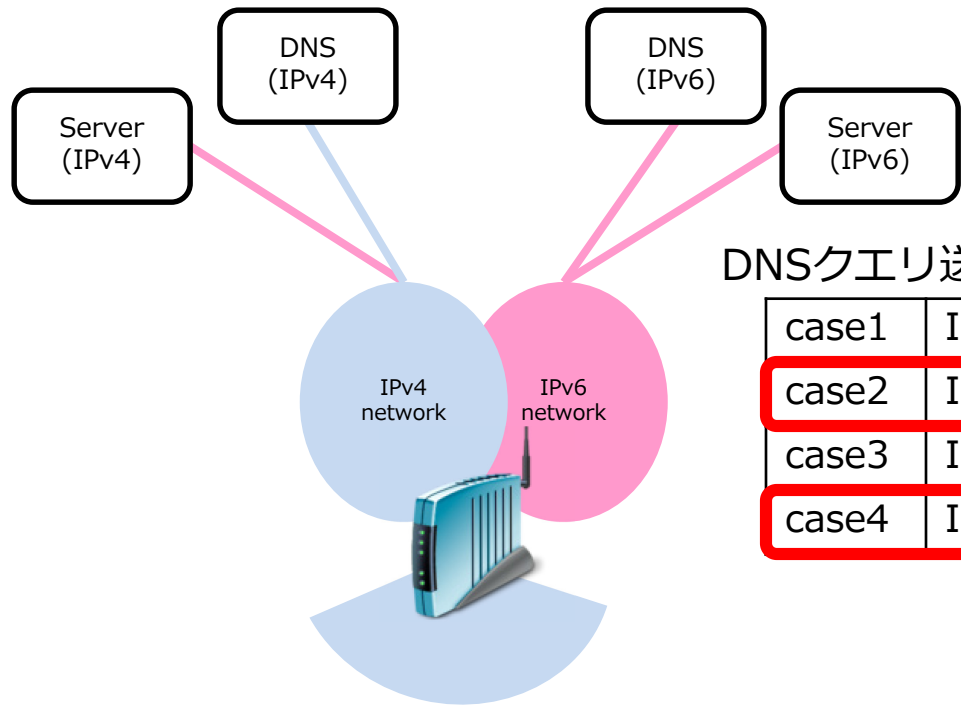
1.3 家庭内ネットワークでの通信不可事例

- リーチャビリティのあるはずのIPv6コンテンツに接続できていない・・・



1.3 家庭内ネットワークでの通信不可事例

- 名前解決は正しく(AAAA)行われているのでしょうか？



DNSクエリ送付パターン

case1	IPv4トランスポート	+	A
case2	IPv4トランスポート	+	AAAA
case3	IPv6トランスポート	+	A
case4	IPv6トランスポート	+	AAAA

いずれかの方法で名前解決できていたのでしょうか。

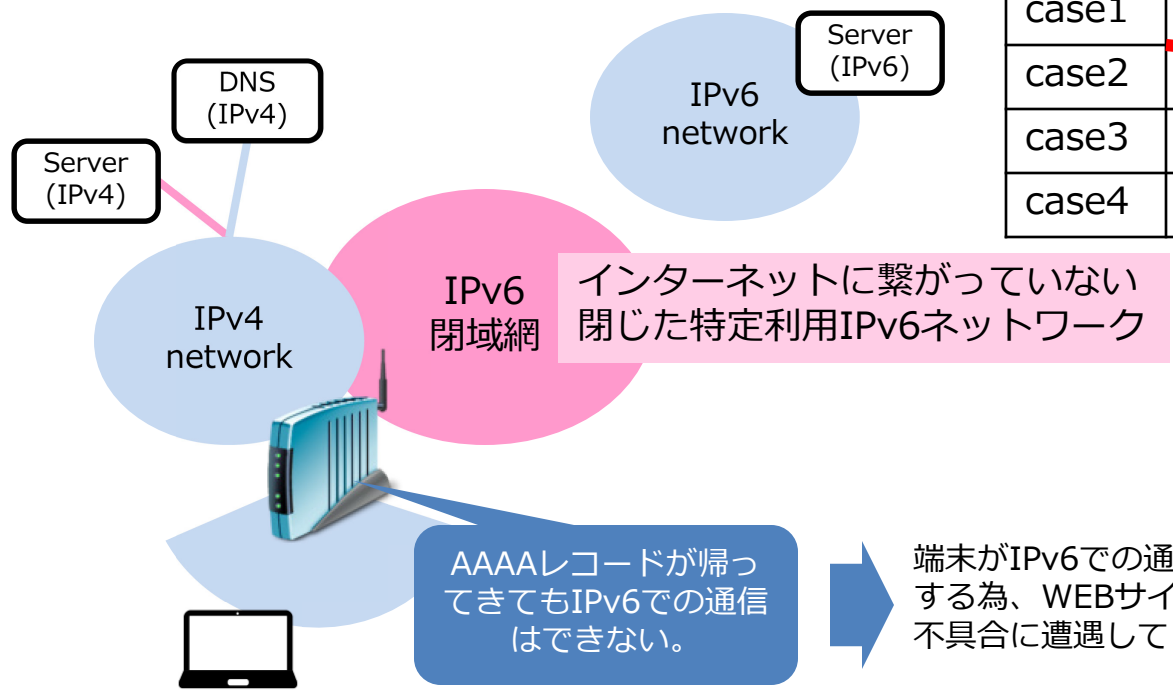
1.3 家庭内ネットワークでの通信不可事例

【解説】

- AAAAフィルタとは。
 - IPv4トランスポートで名前解決がリクエストされた時に、AAAAレコードを削ってAレコードのみ回答する為のDNSサーバに導入されるフィルタのこと。

DNSクエリ送出パターン

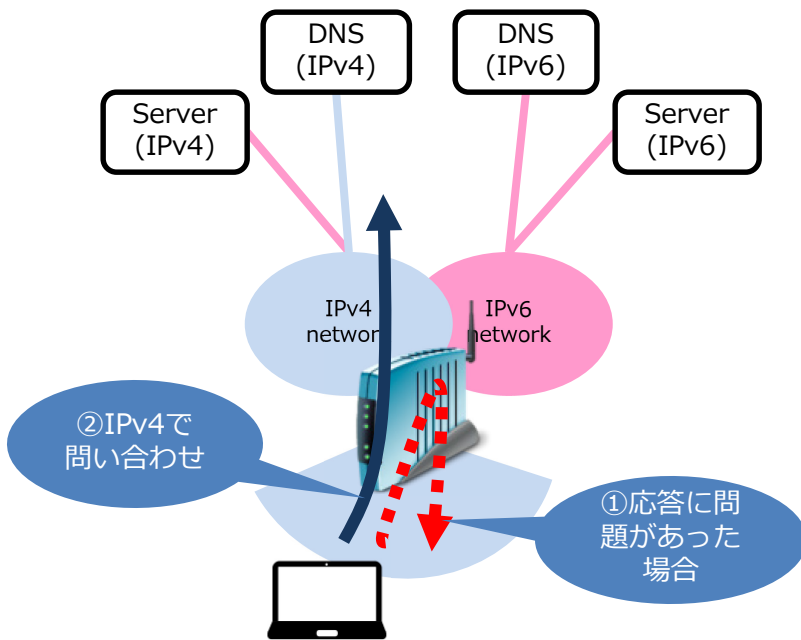
case1	IPv4トランスポート + A
case2	IPv4トランスポート + AAAA
case3	IPv6トランスポート + A
case4	IPv6トランスポート + AAAA



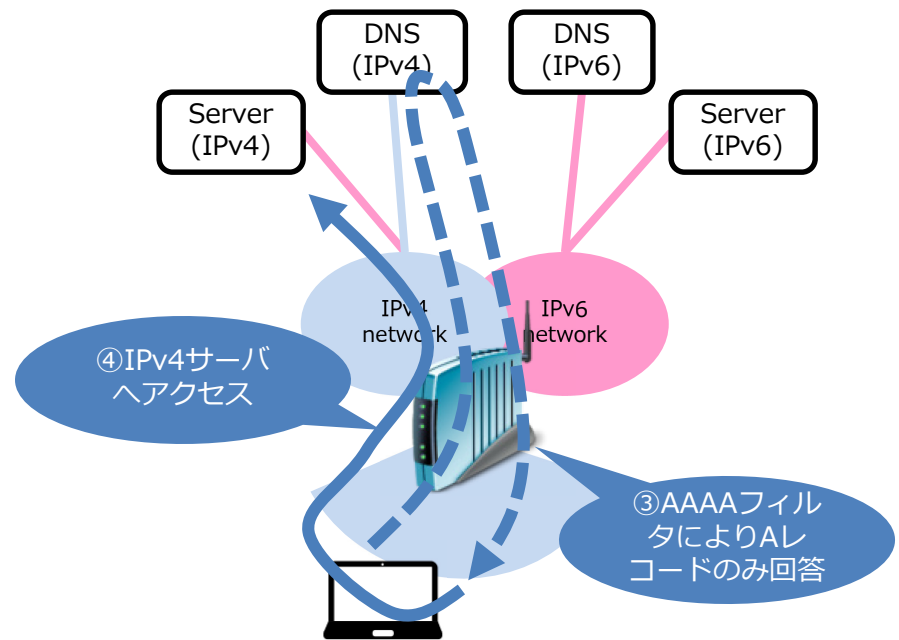
➡ 端末がIPv6での通信を試してからIPv4に“フォールバック”する為、WEBサイト表示に時間がかかるなどの不具合に遭遇してしまう。

1.3 家庭内ネットワークでの通信不可事例

- DNS選択とAAAAフィルタ。



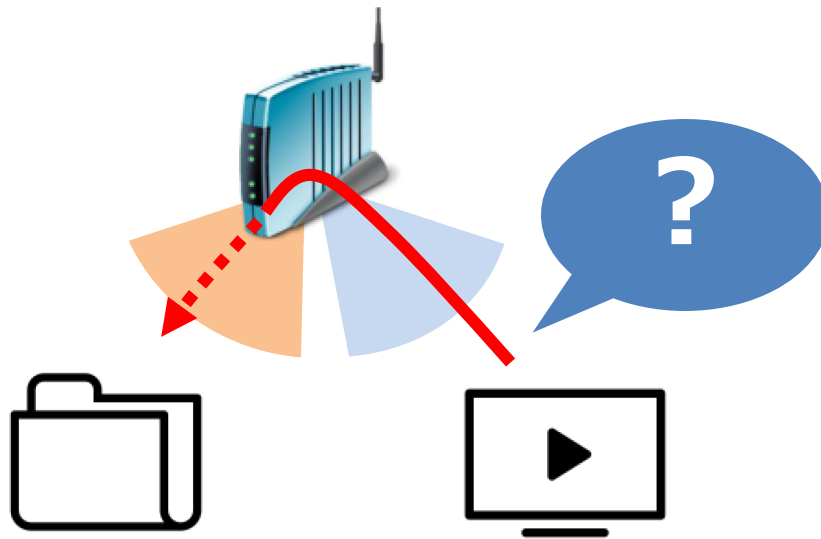
端末が送出したDNSv6クエリ応答で
何らかの問題・・・
→IPv4アドレスにて再度問い合わせ



IPv4トランスポートでのDNS問い合わせの際に
ISPが導入しているAAAAフィルタにヒット
→対象ドメインに対してIPv4で通信を行う。

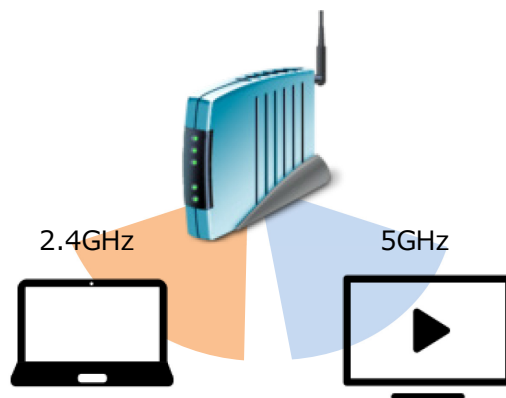
1.4 家庭内ネットワークでの通信不可事例

- ファイル共有/index検索ができない。



1.4 家庭内ネットワークでの通信不可事例

- 各端末の接続メディアは同じでしょうか？
 - 昨今の端末は5GHz対応が広がっている
 - 対してファイルサーバやプリンタなど以前から設置している端末で2.4GHzのみの対応

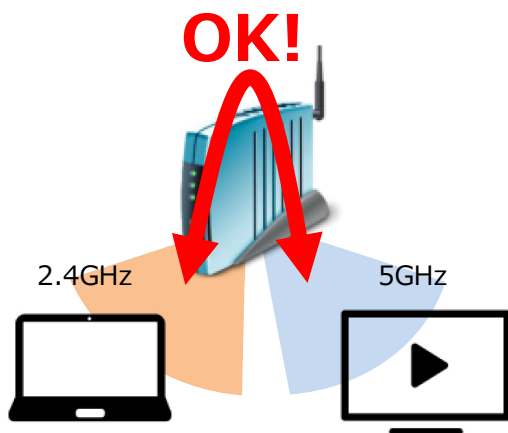


- 2.4GHz/5GHzで両端末がそれぞれの周波数に接続している場合、ルータの機種依存で周波数間をBridgeしないケース。
- 特にわかりやすい例としてAirprintなどプリンタ接続で近隣検索ができない

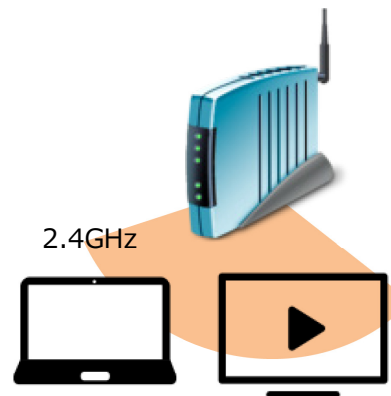
1.4 家庭内ネットワークでの通信不可事例

- ユーザへの案内・インテグレーション時にはユースケースにより該当事象を回避出来るような下記方法を検討

あらかじめユースケースを洗い出し
周波数間でブリッジ可能な機器の利用



より多くの機器が対応している
周波数への変更



目次

- ✓ IPv4/IPv6トロポジ違いによる注意点
- ✓ ホームゲートウェイによるサーバ負荷増大事象
- ✓ 家庭内ネットワークでの通信不可事例
- ✓ **バックボーンでのPath MTU Discovery問題事例**
- ✓ バックボーンでのトラブル事前対策
- ✓ まとめ

- PMTU Discovery問題
 - まだハマってしまっていることあるんです。。

2.1バックボーンでのPath MTU Discovery問題事例

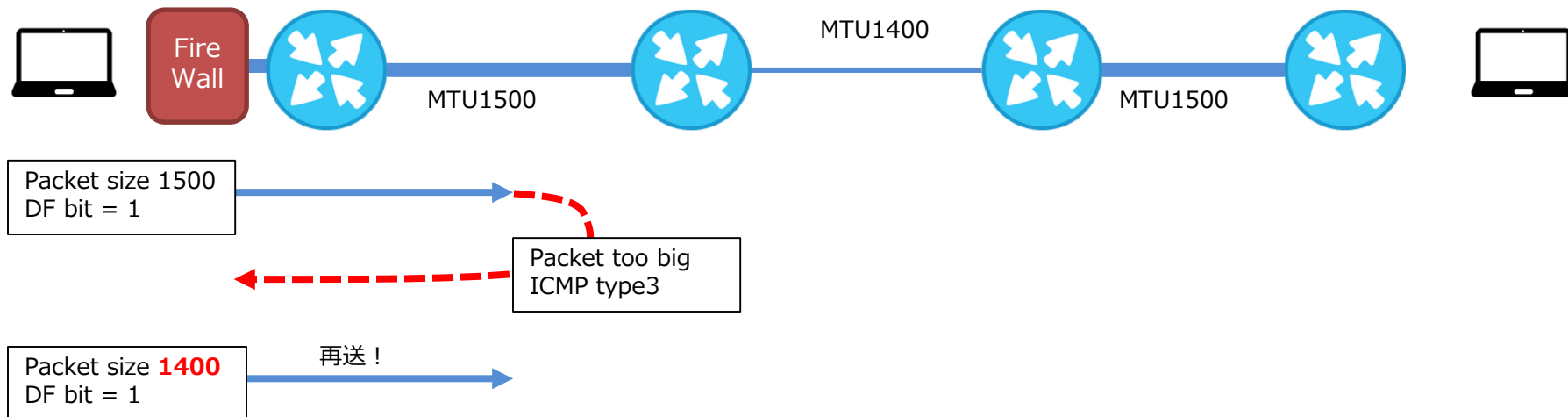
【解説】

- Path MTU Discovery問題とは？
 - ネットワーク上の途中経路にて MTUサイズがパケットサイズを下回った際に再送要求が正常に行われないケース。

2.1バックボーンでのPath MTU Discovery問題事例

【解説】

• おさらい

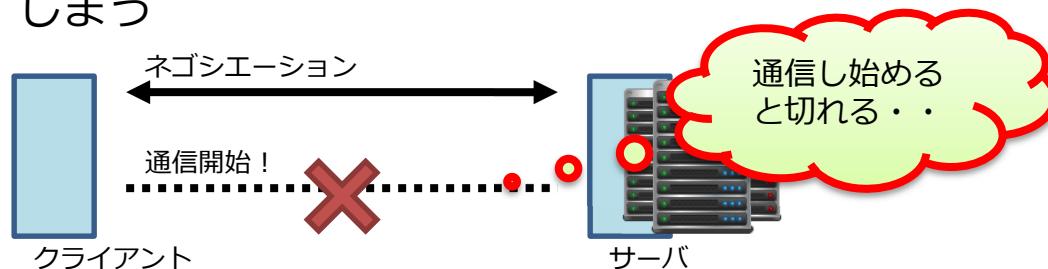


Packet too bigによる正常な再送処理が行われないケースが問題

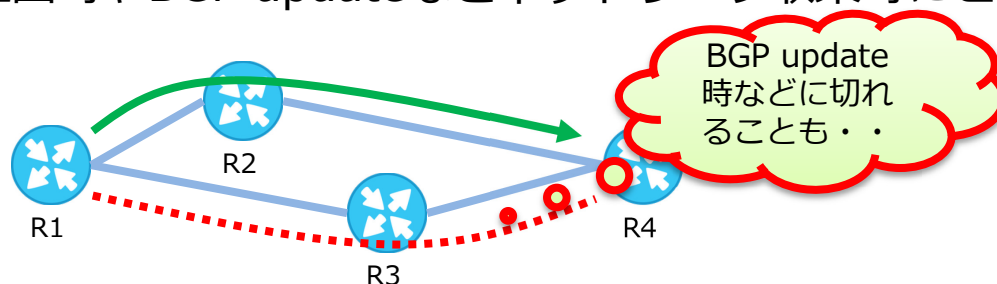
1. 中継ルータによるicmp rate limitation
2. 端末側Firewall機能によるicmp reject
3. 中継SPによるicmp reject

2.1バックボーンでのPath MTU Discovery問題事例

- MTUが適切に設定されていないと・・・
 - 例 1 : ファイルサーバunmount
 - マウント自体はうまくいくがファイル転送/replication時に切断されてしまう



- 例 2 : iBGP切断
 - 迂回時やBGP updateなどネットワーク収束時にピア断



- など痛いトラブルにつながってしまう

2.1バックボーンでのPath MTU Discovery問題事例

- MTU値の適切で“明確”な設定が必要
 - Interface mtuとIP mtu

```
interface GigabitEthernet1/1
  mtu 2000
  ip address 192.168.10.1 255.255.255.0
  ipv6 address 2001:3b8:100:100::1/64
  ip mtu 1500
  ipv6 mtu 1280
end
```

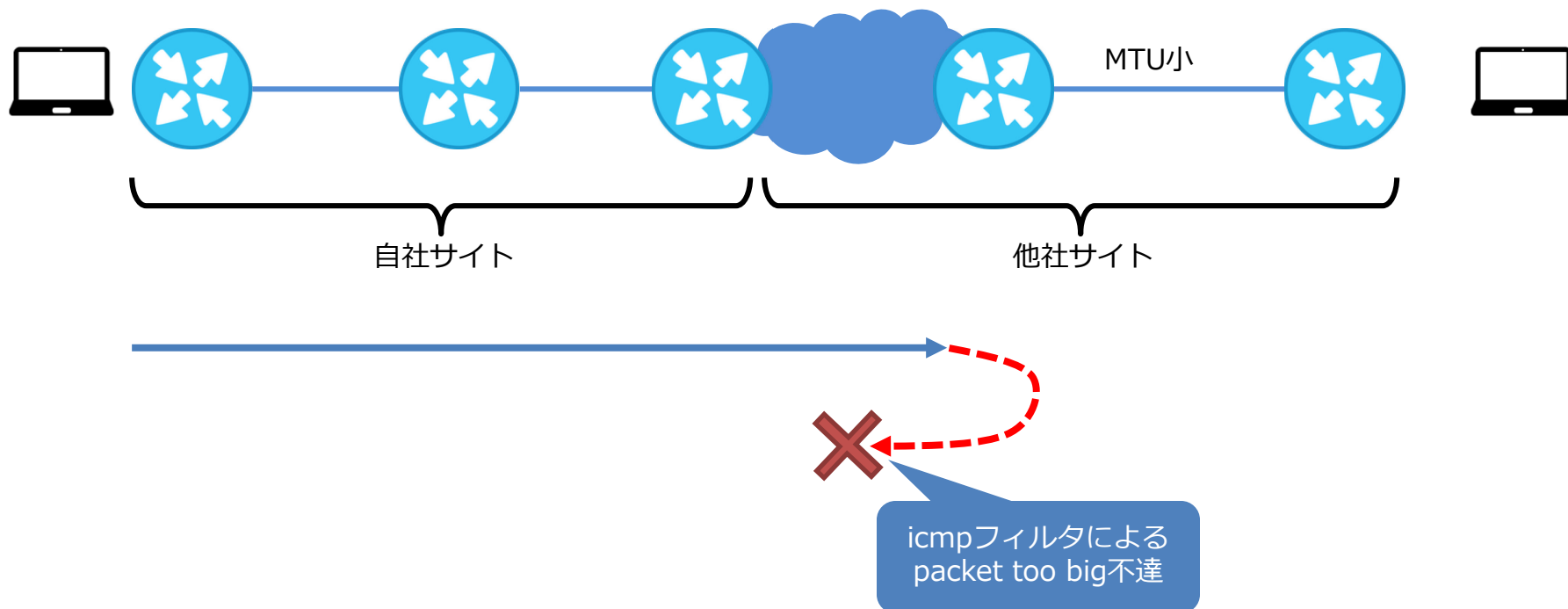
- インターフェース設定mtuとシステム設定mtu

```
system mtu 2000
interface vlan 100
  ip mtu 2000
  ip address 192.168.10.1 255.255.255.0
end
```

※表記している数値自体はすべてのケースに於いて適切なものではありません

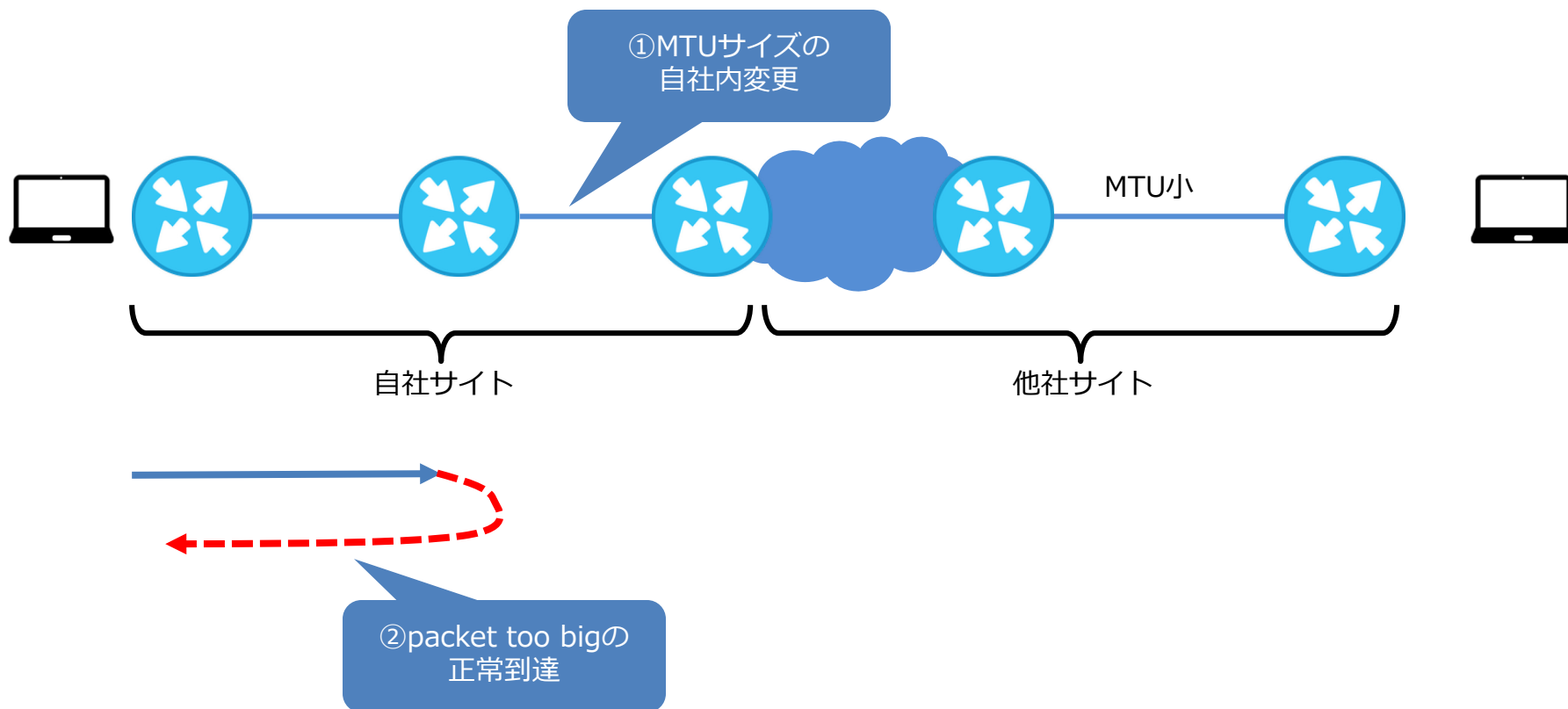
2.1バックボーンでのPath MTU Discovery問題事例

- 遠隔サイトでのPMTU問題発生時対応例



2.1バックボーンでのPath MTU Discovery問題事例

- 遠隔サイトでのPMTU問題発生時対応例



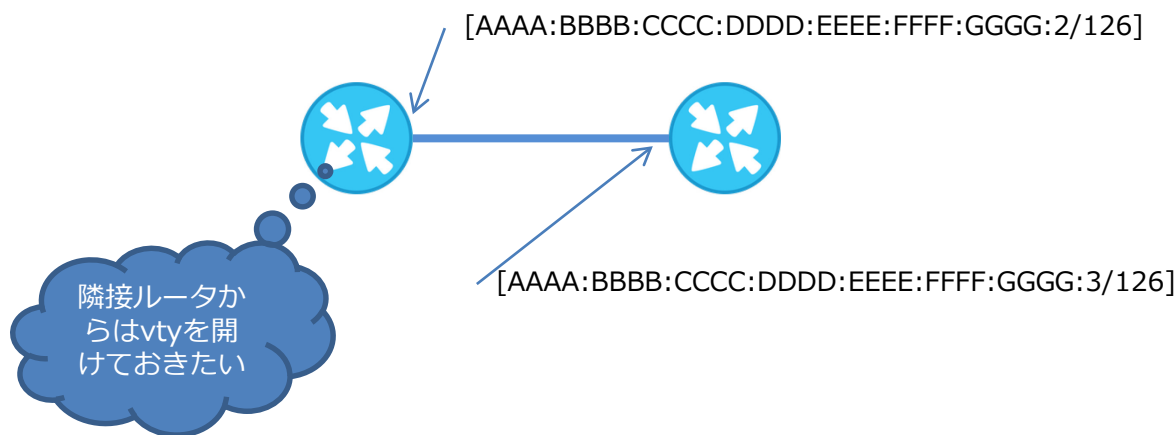
目次

- ✓ IPv4/IPv6トロポジ違いによる注意点
- ✓ ホームゲートウェイによるサーバ負荷増大事象
- ✓ 家庭内ネットワークでの通信不可事例
- ✓ バックボーンでのPath MTU Discovery問題事例
- ✓ **バックボーンでのトラブル事前対策**
- ✓ まとめ

2.2バックボーンでのトラブル事前対策

- アドレッシング&ACL

- 一行あたりが長いACLはソフトウェア処理になってしまったり、ACLとして機能しないような制限に引っ掛かってしまうことも。



特にP2Pセグメントを126ビットで記載、個別にACL穴あけなど行いたい場合などにヒット。
→インターフェース向けパケットの大量流入により負荷増・・・

2.2バックボーンでのトラブル事前対策

- 機器の事前評価と適切なアドレッシングで事前回避
 - とはいえIPv6も節約して使いたい。。
 - P2P用アドレッシング RFC:3627を参照

/64~/112程度が一般的に利用しやすいPrefixサイズ

※ACLに限定したRFCではありませんが、本prefixサイズの適用範囲は他でも有用と考えられる。

2.3バックボーンでのトラブル事前対策

- 回線開通時に疎通が確認できない。
- 切り分けが解り易いケース

– Static接続のケース



確認方法

- NDでの接続確認
- ICMPv6での疎通確認

```
R1#sh ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
FE80::226:99FF:FEC8:D940                   1 0026.99c8.d940 STALE Fa0/0

R2#sh ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
FE80::A60C:C3FF:FEE3:99FE                  1 a40c.c3e3.99fe STALE Fa0
```

– BGP接続のケース



確認方法

- NDでの接続確認
- ICMPv6での疎通確認
- BGPピア状態の確認

2.3 バックボーンでのトラブル事前対策

- 回線開通時に疎通が確認できない。
- 切り分けでハマり易いケース
 - OSPF接続のケース



確認方法

- NDでの接続確認
- ICMPv6での疎通確認
- **OSPFピア状態の確認**

OSPFピアは
GUAの正誤と
は関係ない

2.3 バックボーンでのトラブル事前対策

```
R1#sh run int fa0/0
interface FastEthernet0/0
ipv6 address 2001:3B8:AAAA:AAAA::1/64
ipv6 enable
ipv6 ospf 1 area 0
```

```
R1#sh ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
192.168.10.2	1	FULL/DR	00:00:35	2	FastEthernet0/0

```
R1#sh ipv6 route
```

```
<snip>
OE2 2002:100:100:100::/64 [110/20]
  via FE80::226:99FF:FEC8:D940, FastEthernet0/0
```

```
R1#sh ipv6 route 2002:100:100:100::/64
Routing entry for 2002:100:100:100::/64
  Known via "ospf 1", distance 110, metric 20, type extern 2
  Route count is 1/1, share count 0
  Routing paths:
    FE80::226:99FF:FEC8:D940, FastEthernet0/0
    Last updated 00:01:49 ago
```

Neighborが確立し、
実際に経路も受信できている。

対向のIPv6 GUAが違うケース

```
R2#sh ipv6 interface fa0
FastEthernet0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::226:99FF:FEC8:D940
  Global unicast address(es):
    2001:3B8:FFFF:FFFF::1, subnet is 2001:3B8:FFFF:FFFF::/64
<snip>
```

```
R2#sh run int fa0
interface FastEthernet0
```

```
ipv6 address 2001:3B8:FFFF:FFFF::1/64
ipv6 enable
ipv6 ospf 1 area 0
```

```
R2#sh ipv6 ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Interface ID	Interface
192.168.10.1	1	FULL/BDR	00:00:38	2	FastEthernet0

```
R2#sh ipv6 route
```

```
<snip>
S 2002:100:100:100::/64 [1/0]
  via Null0, directly connected
```

- ✓ IPv4/IPv6トロポジ違いによる注意点
- ✓ ホームゲートウェイによるサーバ負荷増大事象
- ✓ 家庭内ネットワークでの通信不可事例
- ✓ バックボーンでのPath MTU Discovery問題事例
- ✓ バックボーンでのトラブル事前対策
- ✓ **まとめ**

まとめ(1/2)

- IPv4/IPv6デュアルスタック環境でのDNS取扱及び挙動は実装により差が大きく、IPv4オンリーの環境とは違う事を認識すること。
- 機器のMTU設定に於いては各機器明示的な設定を行うこと。

まとめ(2/2)

- 切り分けの際はGUA/LLAの取扱に注意し切り分けパターンに応じて適切な選択を行うこと。
- IPv6の検証については機器選定時にIPv4と同様レベルに行うこと(IPv6は既におまけでは無い)

ご静聴ありがとうございました