

ネットワーク運用からみた オーバーレイ/仮想化技術

NTTコミュニケーションズ株式会社

河野 裕

はじめに

- ・今回の議題では、インターネット運用ではあまり関係ないか、、と、思いがちですが、実は使っていますし、そうでもない近い将来に使い出します。一緒に考えましょう！
- ・ここにいらっしゃる皆さんの経験と知識でより良いものに。
- ・みなさんのご意見いただきたい！

“仮想化” と、インターネット & VPN

■ 日本のインターネット運用者には想像がつきにくい技術

- 日本のインターネットが生まれてからトラフィックの伸びは増加の一方。それを操作するISPは、トラフィック需要にあわせ物理構成を計画的に増設し、物理リンクを使い切る設計をする傾向にある。

— ユーザを束で扱い、トラフィック交換する ⇒ 仮想化の必要がない



一方・・・

- VPNでは当たり前の技術。特にイントリ-型VPNについては複雑化

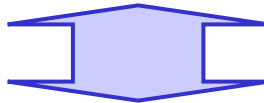
— 大小NWにかかわらず顧客ごとに論理的に分ける必要がある。
⇒ 仮想化は“必須”

“分けるがゆえにVPN”

“オーバーレイ” と、インターネット & VPN

■使っているが、意識はする？しない？

- ・ ユーザへ届ける最終部分は必ずオーバーレイ。プロバイダ事業者によって届けられる。日本のISP技術者はサービスを持っていて、お客様がいる限り必ず使っている
- ・ 対ISP側もサーバや逆側のendにいるユーザにたどり着くためAS間をオーバーレイ。
 - 自網だけでユーザにreachできない (他網でreachできるのがインターネット) ⇒ オーバーレイはしているがあまり意識をしない

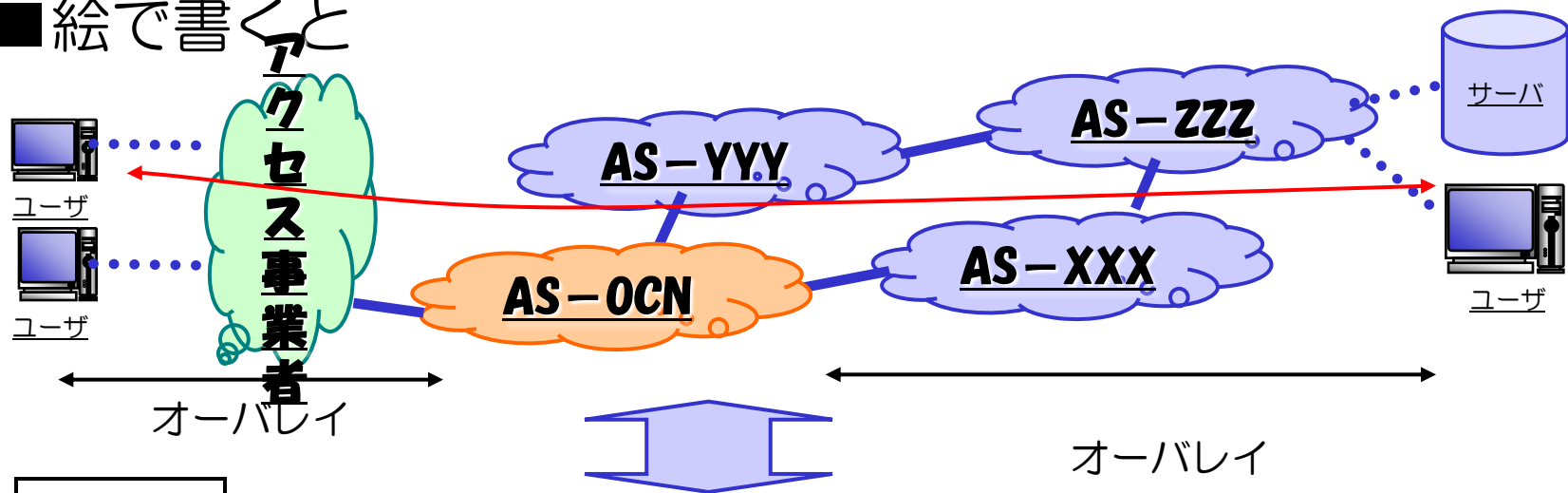


最近は・・・

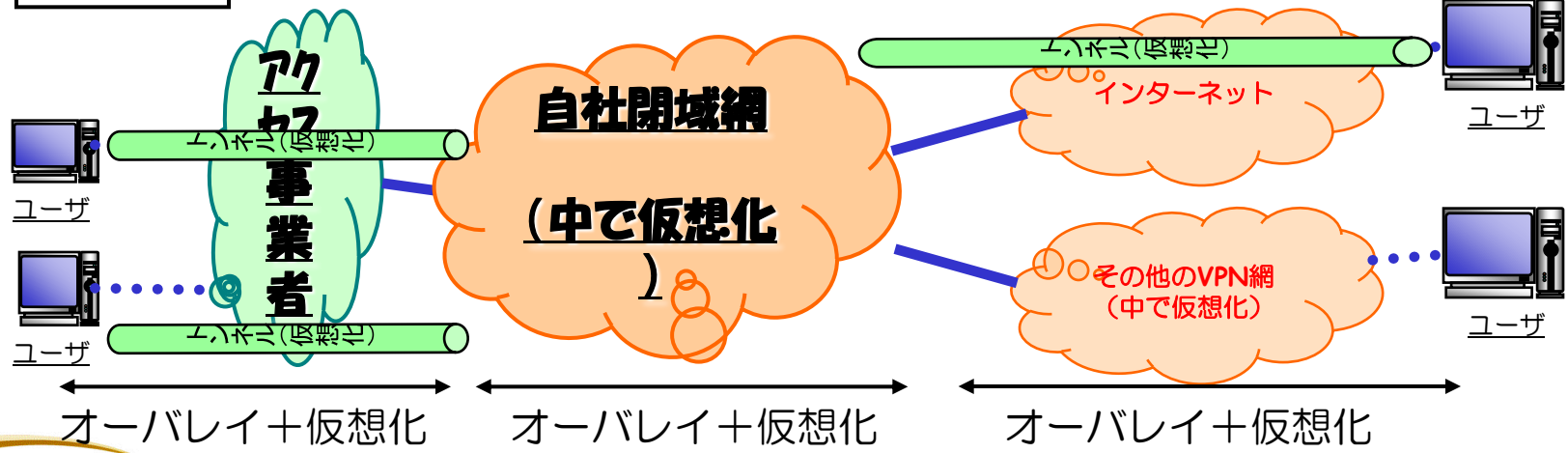
- ・ VPNでもユーザへ届ける最終部分は (あまりやりたくないけど) オーバーレイ
 - 専用線などでユーザにreachする場合もあるが 他社に借り受けてユーザにreachする場合も
- ⇒ 近年はオーバーレイを利用して網を安く構成することが多い

“オーバレイ” と、インターネット & VPN

■ 絵で書くと



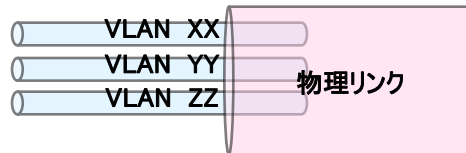
VPNは



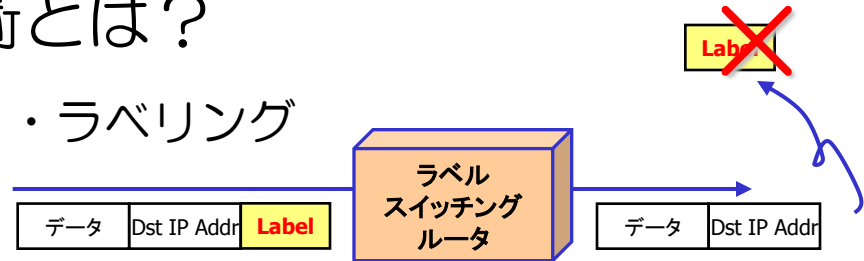
VPNでの仮想化技術

■VPN仮想化する現在の技術とは？

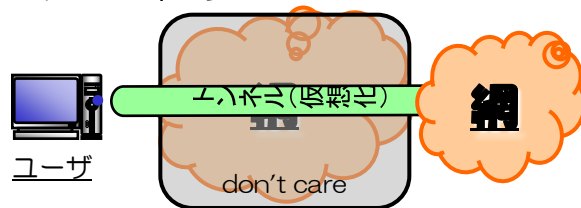
・タギング



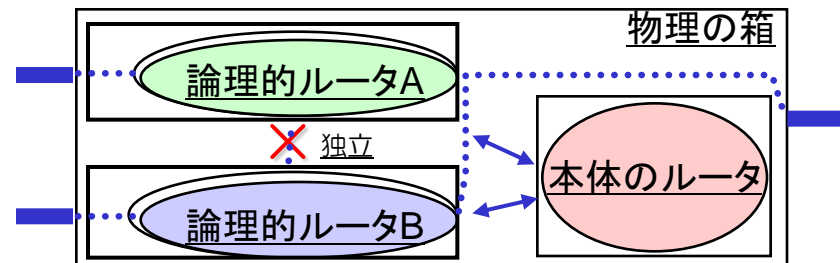
・ラベリング



・トンネリング



・ヴァーチャルルータ (VR)



くるんで隠してVPN

VPNでの仮想化とオーバレイ

■VPNの種類と仮想化技術

IP-VPN MPLS

- mpBGP
- LDP
- VR
- Vlan

ether型VPN

- PBB
- PBT
- VR
- Vlan

インターネットVPN

- IPsec
- L2TP
- vlan
- VR

← **Topic !**

インターネットVPN

- IPsec
- SSL
- SoftEther
- L2TP
- GRE などなど

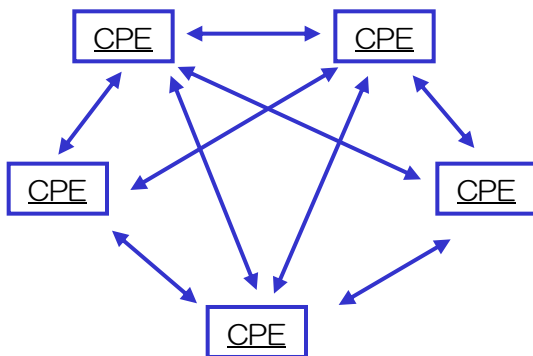
- パケットを何かしらの形で包み自分が通っていくリンクを仮想化し通過ことになる。
- そしてそのパケットが下位レイヤーのプロトコルによってホップしていくことでオーバレイネットワークを流れている。

仮想化とオーバレイネットワークは、VPNでは基本的技術
この技術があるからこそVPNは活躍してる！

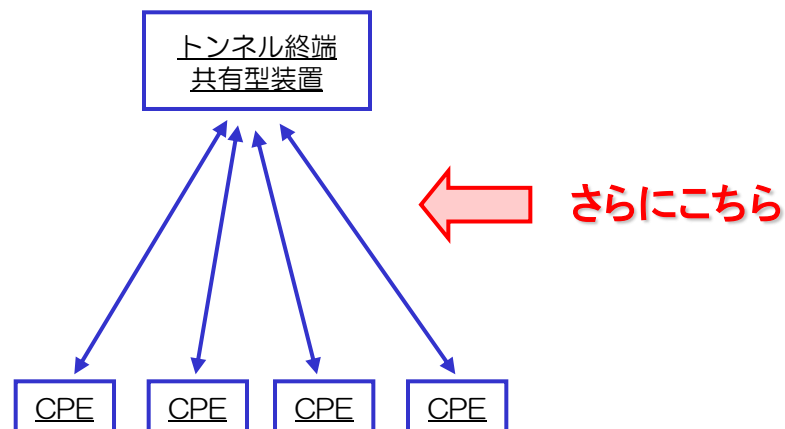
エントリーVPNの種類

■大きく分けて2パターンある。

・フルメッシュ型



・センター集約型



□インフラの最適化/効率化

各種リソースを管理をしつつ、使用効率の向上を目指す。

□物理インフラのコスト削減

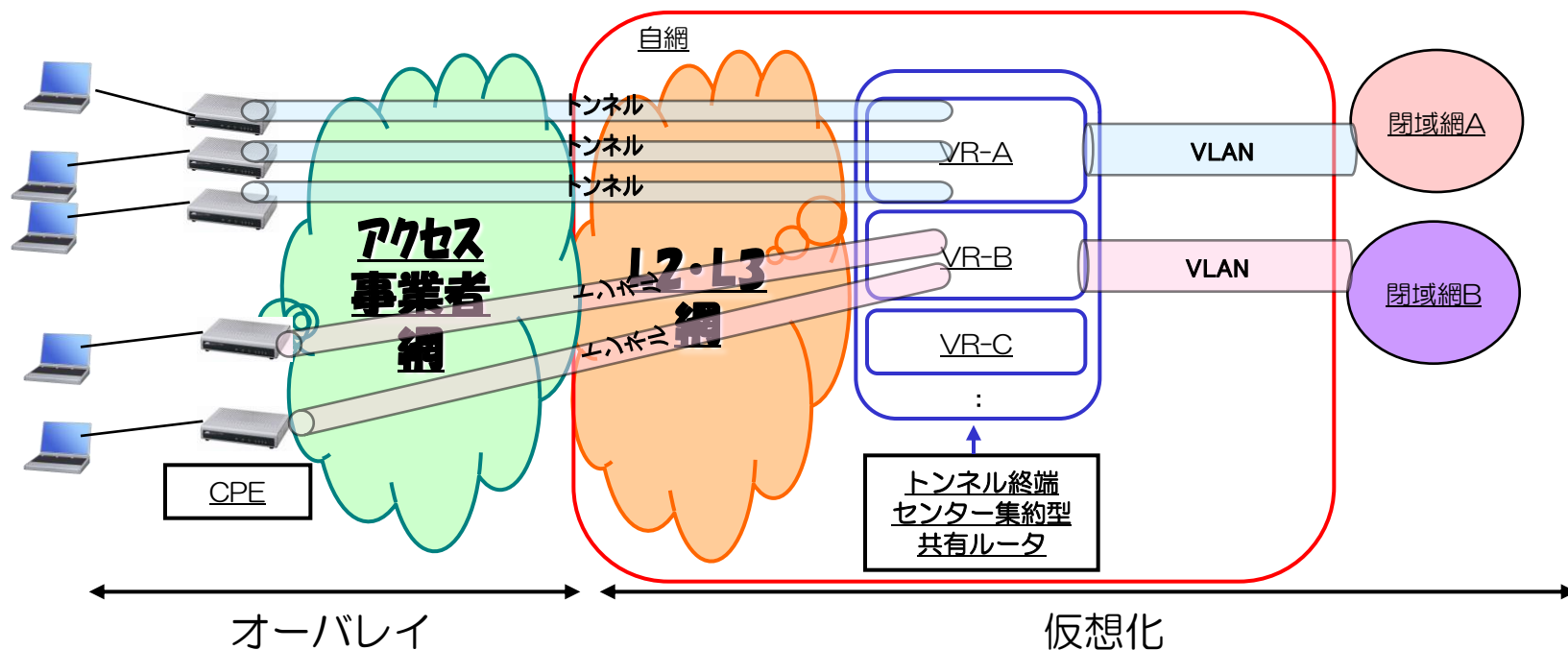
仮想化してたくさん同一物理インフラに収容して、統計多重効果を見込む。

□インプリメントが容易

CPEが小さい、契約が安い、ブロードバンドアクセスが引ければOKで手軽。

エントリーVPNの代表的構成

■ センター集約型エントリーVPNの一例



一般的な装置の機能：

□ 一般的なトンネル終端型装置、共有ルータ

ー複数のVR収容

ー複数のトンネル終端

□ CPE

ースループットは低

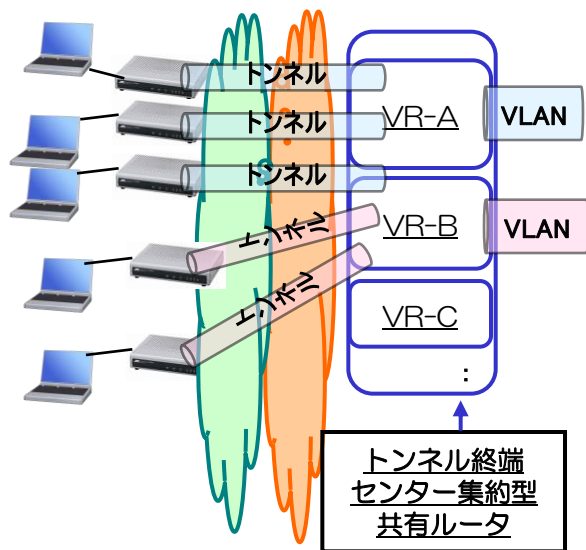
ーvlan拡張はしてないものが多い

ーリソースが別れているかは装置依存

ーできるだけ機能はなくし、コストを安く

エントリーVPNの仮想化での問題

■仮想化装置の収容効率と安定性のジレンマ①



◎装置故障：

□装置の物理故障でのインパクトが大きい

□論理的に複雑なため、故障被疑個所の特定が難解
—HW確認→VR確認→トンネルチェックして、、、
⇒原因判明の長期化

□論理故障やバグを引くと、すこぶるまずい状態に

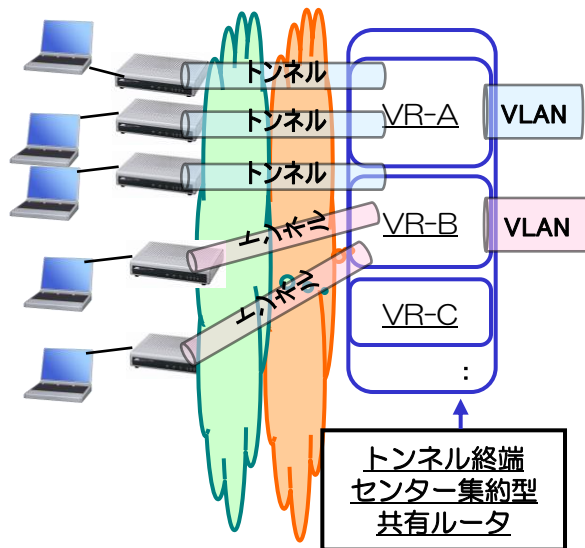
⇒最悪の場合、実網デバッグ&解析状態に。

仮想化装置の安定性は最重要課題

- ・ ハングするぐらいならすっきりダウンが望ましい
- ・ 装置のスムーズな切り替わり。装置内情報の同期が◎

エントリーVPNの仮想化での問題

■仮想化装置の収容効率と安定性のジレンマ②



◎装置内リソース管理：

- 設計し運用する際に装置内リソース配分を考慮することが通常のL2,L3装置に比べ、数倍の苦労がある。
 - ーどんなリソースがあるのか、もれなく管理できるか？
 - ーそれぞれの設定上限は？
 - ー安全な設定の値は？
 - ー全設定値のバランスは？
 - ーそれぞれが上限を超えた場合発生しえる問題は？
- アロケーション問題
 - ーリソースの分け方に基準がないため頻りにポインターエラーや、クラッシュに出くわす

■リソース管理の機構は必須

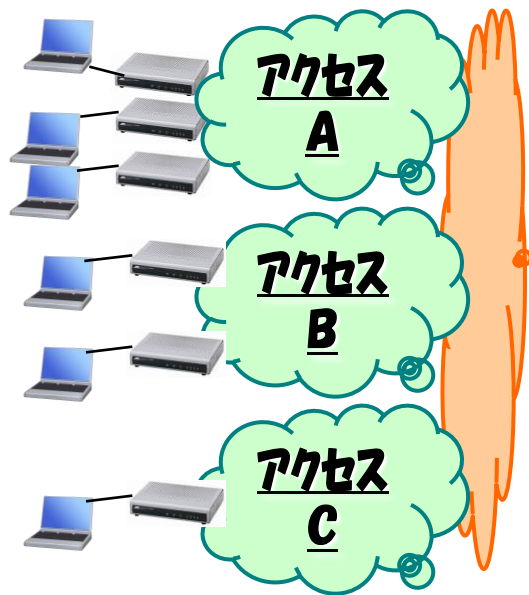
- ー標準化の段階で、できる限り管理できるよう定義したい
- ー複数ある管理項目をシンプルに管理できるインタフェースがほしい

■メーカーでここまでバランスをとる事を期待します。

- ーハードウェア設計にまで踏み込んだ研究開発をお願いしたい！

エントリーVPNのオーバレイでの問題

■アクセス網との戦いの日々①



◎新網の登場と接続

- オーバレイをした上レイヤでは、アクセス網がどうあれサービススペックを保たなければいけない！

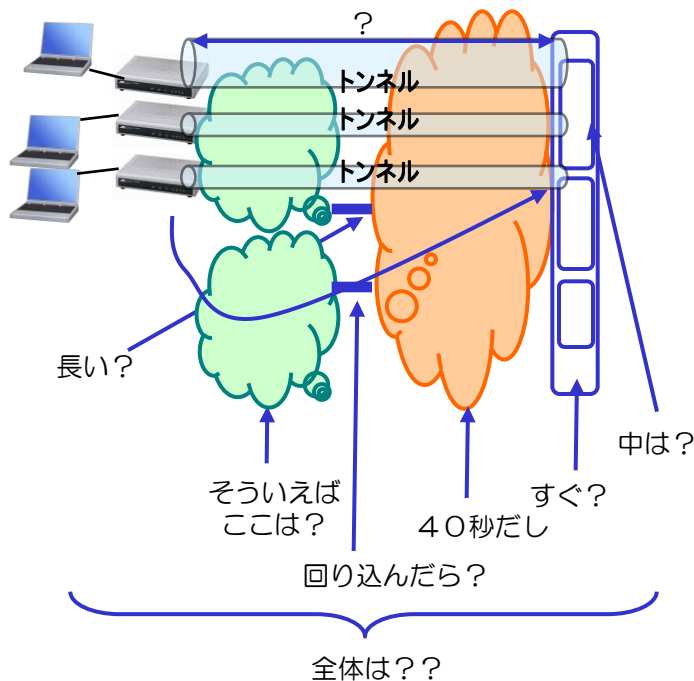
◎運用後の問題

- アクセス網内の問題にも対応しなければならない
 - ー輻輳
 - ーRFCの合間

下レイヤのスペックは、大きく上レイヤのスペックに影響します
現状のアクセス網はベストエフォートを前提で考慮しなければならない。

エントリーVPNのオーバレイでの問題

■下レイヤとの戦いの日々



◎通信品質管理：

- ダウンタイム設計
 - 下位レイヤを想像して設計しているのが現状
 - 新しいサービスのせたらどうなるの？
- 故障時事象の魔
 - どこがどう壊れたから何秒きれたのか？
- 想定外の事象の魔
 - 1箇所が予想より長く切れたら？

オーバレイ技術を作る際には、

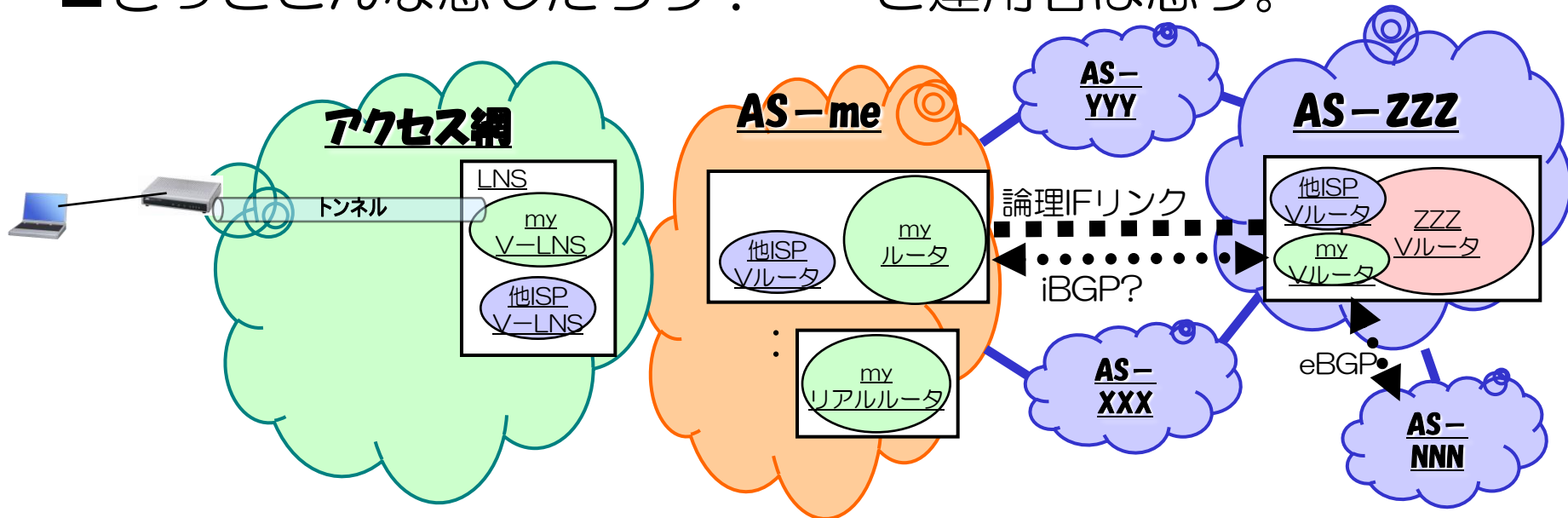
- ・ 上位レイヤには、下位レイヤの状態がわかる仕組みがほしい。

もしくは

- ・ 下位レイヤに、上位レイヤに伝達する仕組みがほしい。

仮想化とオーバレイネットワークの将来

■ きっとこんな感じだろう！ と運用者は思う。



- 仮想化を自網以外に導入した場合、
 - ◎ そのポイントで状態確認ができるので、運用性の向上につながり、増えていくであろうオーバレイ部を減らすことができる。

■ 物理が自網にない中でセキュリティーホールにどう対処するか？

将来の仮想化とオーバレイネットワークに望むもの

■仮想化

- 装置依存にならないこと
ーリソース管理に気を配って、情報を可視化して！

- 仮想化の技術を乱立せず、ある程度数を絞って、
ー組み合わせる仮想化技術間のインターワークも考慮にいられて作ってほしい

- 自網以外にルータができるなら・・・
 - ◎ コントロールポイントが増えることになる。
 - Vルータでも通常のルータと同様のさわり心地を！
 - * 運用においては、お互いの連携が重要になります！

将来の仮想化とオーバレイネットワークに望むもの

■ オーバレイ

- 上位レイヤには下位レイヤを感じ取る仕組みがほしい。
もしくは、下位レイヤが情報を出す仕組みを作り、上位レイヤが感じ取る仕組み
→ 他網に入った時に、下位レイヤ情報を集めてくる
→ 下位レイヤのStateを記述するための制御用パケットを定義、とか。
- 現状は、下位レイヤはほとんどがベストエフォートなので、
それにのせる前提で、オーバレイの実装を進めてほしい。

■ 両者を総じて

- シンプルに設計できるように考慮してほしい
 - ー そもそもかぶせる技術、通常で2倍以上は難しい
(通常のルーティング+仮想化+内部ルーティング・・・)
 - ー メーカーもベンダーも、設計者も苦労します。一番苦労するのは運用者！
 - ー トラブルが起きたら本当にわからなくなります。

*あまり難しすぎると誰も使えなくなってしまいます。

最後にまとめとして

・ 今までの運用経験上・・・

- －運用者の自分としては、現状の技術は好きではない・・・
 - －わかりづらい
 - －怖い
 - －夜寝れない(電話には出ます)

- －設計者の自分としては、どちらも
 - －運用者の気持ちが半分
 - －設計者として、がんばるほどみなさんに恩恵があるのでやりがいはある
 - －下位レイヤを意識しない未来の技術に期待
 - －テストプロジェクトに参加したい！

- －1個人ユーザとしては、
 - －ユーザにメリットがあれば、やってほしい
 - －安くなっているのだよ、といわれてもピンとこないかもしれない。
 - －あまりわからないのなら。。壊れないほうでお願いしたい。

オーディエンスの皆様、研究者の皆様はどう感じるのでしょうか？

おわります