

IPv6の真の普及に向けて ～残る課題と解決への道筋～ ちょっとアップデート版



2024年7月

NTTコミュニケーションズ株式会社

イノベーションセンター 担当部長

シニア・テクノロジー・アーキテクト / エバンジェリスト

博士（工学） 宮川 晋

shin.miyakawa@ntt.com

自己紹介

宮川 晋 (みやかわ しん)

NTTコミュニケーションズ株式会社
イノベーションセンター (本務) / 第二ビジネスソリューション部 (兼務)
担当部長
シニア・テクノロジー・アーキテクト / エバンジェリスト

来歴と主な所属

平成7年 東京工業大学 博士 (工学) 学位取得 同年にNTT入社
NTTソフトウェア研究所、NTT MCL (シリコンバレー)、NTTコミュニケーションズ 技術開発部
慶應義塾大学SFC研究所上席研究員(客員)

主な研究関係の業績

IETF RFC6888, 3769, 4241, 4925 IPv6、Carrier Grade NATなど
BSDを256倍つかうための本 (アスキー出版局)
はやわかりPCUNIX (共立出版)

西麻布のバーでNTT Comの宮川エバに聞いたテッキーなお話

<https://ascii.jp/elem/000/000/988/988432/>

Google IPv6 Conference 2008

- <https://www.youtube.com/watch?v=mZo69JQoLb8>
- Google IPv6 Conference 2008: What will the IPv6 Internet look like?



<https://ja.wikipedia.org/wiki/ヴィントン・サーフ>

ヴィントン・グレイ・サーフ（**Vinton Gray Cerf**^[1], [1943年6月23日](#) - ）は**アメリカ合衆国**の**計算機科学者**であり、[ロバート・カーン](#)と共に^{[4][5]}**インターネット**と**TCP/IPプロトコル**の創生に重要な役割を演じた「**インターネットの父**」の1人^{[6][7]}。その功績により、[アメリカ国家技術賞](#)^[1]、[チューリング賞](#)^[8]、[大統領自由勲章](#)^[9]を受賞（受章）し、[全米技術アカデミー](#)会員にも選ばれている。通称は**ヴィント・サーフ**（**Vint Cerf**）。

Mobile World Congress 2018

- McLaren's Keynote at MWC 2018 with Dr. Shin Miyakawa from NTT Communications on 27th Feb 2018 at Barcelona Spain
- <https://www.mobileworldlive.com/on-stage/mwc/keynote-mclaren-formula-1-driver-fernando-alonso-and-zak-brown/>



<https://ja.wikipedia.org/wiki/フェルナンド・アロンソ>
フェルナンド・アロンソ・ディアス（**Fernando Alonso Díaz**, [1981年7月29日](#) - ）は、[スペイン・アストurias州オビエド](#)出身の[レーシングドライバー](#)である。[2005年](#)に、当時のF1史上最年少[ドライバーズチャンピオン](#)記録を樹立し、翌[2006年](#)には連覇を達成した。また2018年にはF1と並行して[ル・マン24時間](#)にも参戦し、総合優勝を収めた。2019年に[ル・マン24時間](#)を連覇し、2018/2019シーズンの[FIA世界耐久選手権](#)LMPドライバーチャンピオンを獲得した。

- <https://www.as-web.jp/overseas/486286>
- **ラップダウンから優勝争いへ。30万人を沸かせた琢磨10度目のインディ500「今日は喜んでもいい3位」**
 - 2019年 5月 INDY 500 佐藤琢磨選手 三位
 - 佐藤琢磨選手の左奥のほう。。



5

ウォーリーを探せ状態ですが。。

- [「優勝に値する4位」苦しみ抜いた大嶋和也がhttps://www.as-web.jp/super-formula/956801SF第5戦SUGOで結果を残す。チームスタッフに涙 | スーパーフォーミュラ | autosport web \(as-web.jp\)](https://www.as-web.jp/super-formula/956801SF第5戦SUGOで結果を残す。チームスタッフに涙 | スーパーフォーミュラ | autosport web (as-web.jp))
- <https://www.as-web.jp/super-formula/956801>

豊田章男
トヨタ自動車会長



私

IPv6 対応ガイドライン 令和4年3月

総務省 IPv6 対応ガイドライン

https://www.soumu.go.jp/menu_seisaku/ictseisaku/ipv6/index.html

これをつくってからそれなりの時間が経ちました。

本質的にはこのガイドライン作成時の状態とあまりかわってるとはおもっておりませんが、先々週のIETFでも大事な進展がありましたので、そこをまじえたうえで、

IPv6が隅々まで普及するためには？

をテーマにお話をしてみたいと思います

実は「v6でもNATをつかえるように。。」という話が中心です

v6のサービス自体は普及したんですよ

ISPサービスや携帯電話サービス、v6が普通に。

- あちこちで言われておりますので改めていうまでもないことですが、IPv6の接続サービスは我が国において普通になりました
- 光ファイバーでの有線接続サービスや、キャリアの携帯電話、普通にv6が降ってきます
- っていうか、v6がベースでv4はすでにAs a Service状態になりつつあります

- AkamaiさんなどのCDN事業者も積極的にIPv6対応が進み
- Facebookさんなどのコンテンツ事業者さんもv6対応が進んでいる

- ので、コンシューマー市場としてのISPネットワークでは、IPv6がトラフィックボリュームの半分以上に なったりしています
- 末端のFlet's に至ってはv6がベースプロトコルですし

- 大変長い時間がかかりましたが、やはりv4アドレスが枯渇してからというものきちんとv6の通信サービスが普及してきたわけです

- でも一方で。。。

企業網にはさっぱり入っていかない

- 家庭やコンシューマーのほうのインターネットではガンガンv6化がすすんでいます、
- 会社のネットワークには全然導入される感じがしないです
- マイクロソフト社社内とかはずっとずっと昔からv6らしいですけど

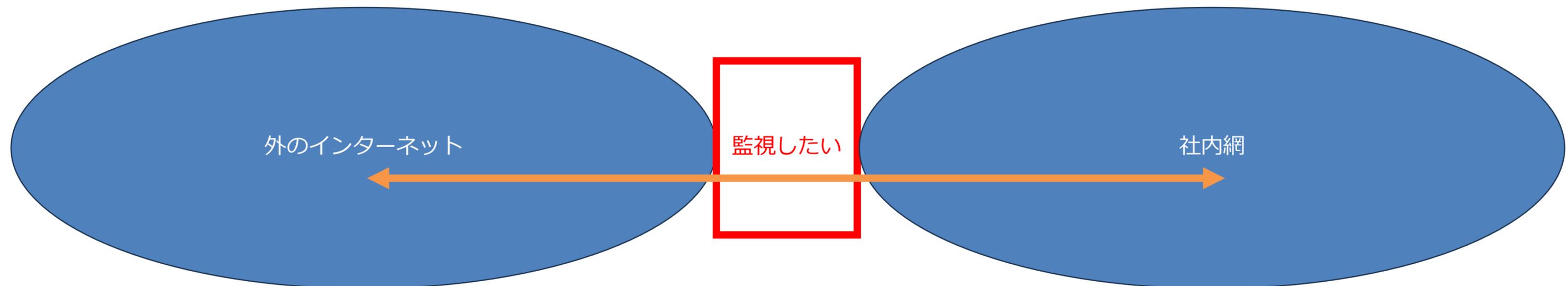
- **なぜ入らないのか？ どうしたら入るのか？ ってか、 いれないといけないか？**

- ってあたりをみていきたいとおもいます

社内網にv6は必要なのか

必要かっていわれるとなくとも大丈夫なんで。。。。

- そもそもIPアドレスがv4プライベートであることがほとんどです
- すると企業網「内部」の通信はそれで十分だし
- **セキュリティ対策的にはProxyなどのいわゆるMiddle Boxを通過させて通信を監視するほうがいい、とま**
でいわれていることもあり
- v6にしなきゃいけない、理由がまったくない、というかしないほうがいいという結論になりがち
 - エンドツーエンドで暗号化されると困るという話になる
- そりゃ、はいらないですよええ。。。。



プリンターとかファイルサーバーとか

- 社内からしかアクセスしてほしくないプリンターとか、ファイルサーバーとかにv6のグローバルアドレスが付いていると逆に不安
- 調べてみると、プリンターのv6対応は昔より後退しているのではないかと思えるくらい
- 「プライベートアドレス」が安心の材料になっている
- IPv6化してもULA (Unique Local Address) をプライベートアドレスとして使えばいいのではないか？

1600万という数字

- IPv6にするモチベーションは、アドレスが足りないというときにどうするか、ということに尽きます
- セキュリティが高くなるとかそういうのはわりとどうでもいいってことです
- 10.0.0.0/8 というアドレス空間は、約1600万となりますが（より正確には167772160）、社内でこの数を超えるアドレスが必要な場合にはv6が自然な選択となります
- そんなことあるの？っておもわれるかもしれませんが、IoT機器とかの進展を考えるとあながちあり得ない数字ではありませんのでそれはそれで自然にすすみますが
- とはいえ、大多数の企業にとって1600万個もいらないでしょ、というのも事実です
- じゃ、v4でいいじゃないか、ってことになりがちです

v6普及に向けてまだ足りない技術

v6にもNATがいるんじゃないか…

- もともとは、v4アドレス枯渇対策としてv6導入までのつなぎとして考案されたNATですが、副作用はインターネットのあちこちにみられます
- v6にもNAT（NAPTにしるNPTv6（これらについては後述）にしる）がいるのではないかと議論は定期的にIETFでも起きますが、なかなか公式にIETFのほうで方針を転換することにはなりません
- 実際にはv6のNATの実装はそこら中であって使われています。IETFって「デファクト」スタンダードじゃなかったっけ、っておもうんですが。。。

v6における二つのNAT

IPv6では、二種類のNAT (Network Address Translation) を想定しておく必要があります

(1) NATv6 (Network Address Port Translation IPv6)

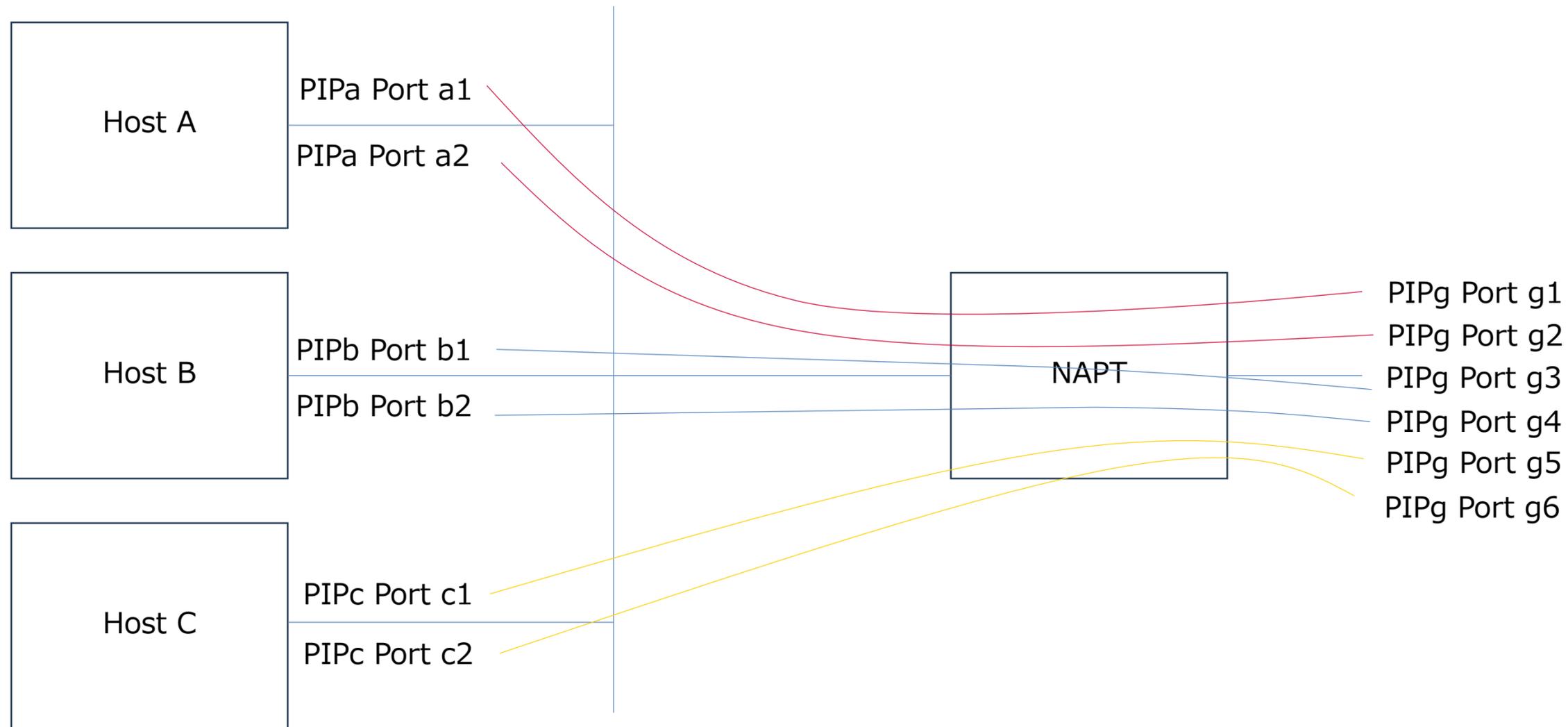
v4で多く使われているNAT。多くの場合ですが、一つのGlobal v4 アドレスに対して、「裏側」にある多数のv4のホストからのTCP、UDPのそれぞれのPortを、その外側のアドレスのPortにマッピングすることで、多数のホストをあたかも一つのホストに見せる技術

(2) NPTv6 (Network Prefix Translation IPv6)

<https://datatracker.ietf.org/doc/html/rfc6296> IPv6-to-IPv6 Network Prefix Translation

に規定されるプレフィックス変換。アドレスが1:1で変換されるのでよくいわれるNAPTの弊害が少ない
現在Experimentalとしての規定ですが、先々週にプラハで開催されたIETF118にてStandardへの変更が提案

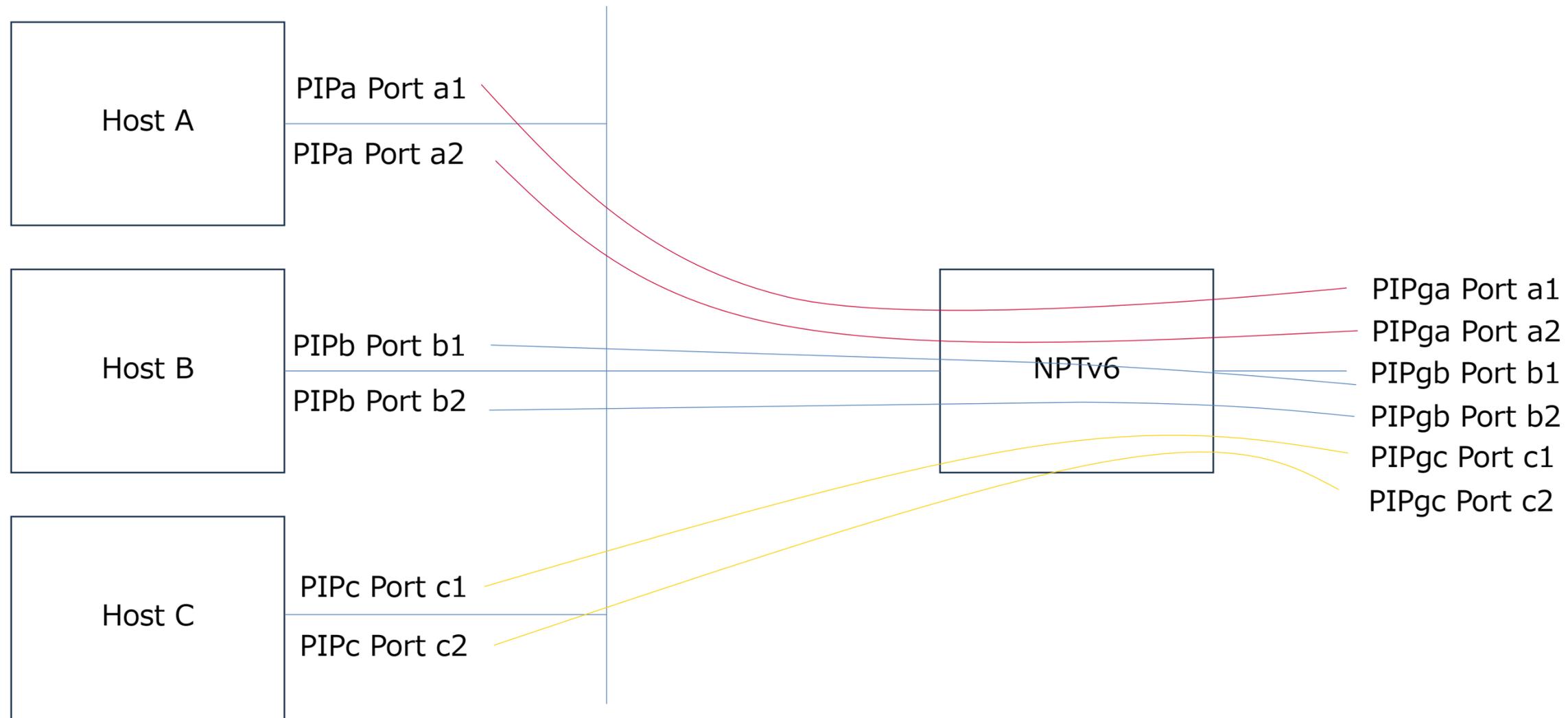
NAPT



NAPTの裏側のホストのそれぞれのアドレスPIP_xのTCPあるいはUDPの各ポートをNAPTの外側のアドレスPIP_gのポートと組にすることで外部との通信を実現する

NAPTの外側のポート番号の数（2バイト分すなわち65536個）を使い切るとそれ以上の対応はとれない。これをNAPTのポート数あるいはセッション数制限という

NPTv6 (あるいはNAT66)



IPv6 のアドレス構造のうち、上位64ビットのプレフィックスを変換する
(CRCが壊れないように下64ビットをいじるというトリックがある)
プレフィックスを変えるだけなので1:1対応となる。ポートは変わらない

NATが欲しい場面というのは

v6でNATが欲しい場面というのは

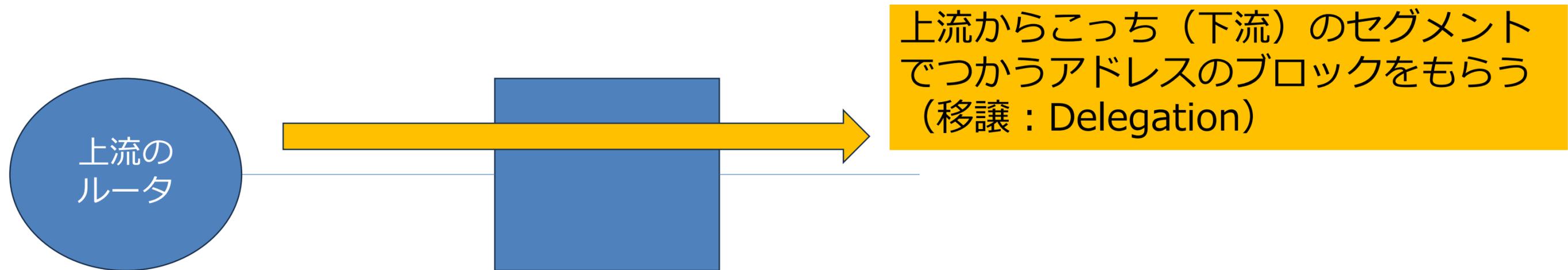
- ノートパソコンでハイパーバイザーを使ってる場合
 - Prefix Delegationをうまくつかうとこの場合は解決できることがわかってますが。。
- K8Sでコンテナを使ってる場合
- ロードバランサーをつくりたいとき
- お手軽なISP多重化をしたいとき

などがあります

- 意外かもしれませんが、フレッツで「ひかりTV」を御視聴の皆様、もれなくv6NAT使ってます
 - 閉域網プレフィクスとの間で橋渡しが必要だったんで。。NPTv6 (NAT66) なんですが、つくっちゃいました (遠い目)

Prefix Delegationをもっとつかおう

- 要するにアドレス空間は沢山あるんだけど、うまく「配る」方法をもっと工夫しないといけない
- Prefix Delegationっていう概念があるわけですが（下図参照。私が世界で初めて提唱してRFCにしたんですよ（自慢です））、これをISPの接続のところだけでなく、あちこちのLANでも使ってアドレスを配れるようにするとずいぶん違います。



Prefix Delegation Per Host

DHCPv6 PD Per Host (ホストのそれぞれにプレフィックスを配る) というアイデアが提案されています

draft-ietf-v6ops-dhcp-pd-per-device

Using DHCPv6-PD to Allocate Unique IPv6 Prefix per Client in Large Broadcast Networks

5 November 2023

ネットワークの各ホストに対してプレフィックスを配る

ということは、

すなわちホストの「なか」とか「うら」でそのプレフィックスを使ったサブネットを構成してよくなる

これをつかうことで、NATを使わなくてよくなるケースが多々あるという主張です

Prefix Delegation Per HostをつかってNATを排除



PD Per host はとても良いアイデアです

このPrefix Delegation Per Hostというアイデアはとても良いアイデアだと思います

v6の原則にも即しているし、うまくうごくとおもいます

が、v4のやり方に慣れた人にはちょっと扱いづらいのも事実だし、
これからこれを普及させていくには相当の時間がかかってしまいます

ですので、v6NATを使えるようにして、v4と同じやり方、も許しつつ、
可能な限り、この新しいPD Per Hostをつかえるところではつかっていく
というのがよいやりかたなのではないでしょうか

ULA (Unique Local Address) まわり

ULAは、プライベートアドレス、ではない。いまは。

- ULA (Unique Local Address) は、プライベートアドレス、ではありません
- そうじゃないのですが、実際にはNAPTv6をつかってプライベートアドレスとして使われる例が多い
- VMWAREにしる、K8S環境にしる。。。
- IETFでも議論百出なのですが、私としては、v6のもともとの思想とは相いれないということはわかったうえで、現状を追認すべきだと思っはいるのです。DHCPv6 PD Per Hostは理想的ではあるのですが、普及まで時間がかかりすぎると、簡易マルチISP接続には使えない。。
- しかし、アドレス選択ルール上も、**Global v6、Global v4**ときて、次が**Private v4**で、**そのあとにULA**です。ので、いろいろなときにせつかくv6があっても使われないこととなっていて、問題があります
- 社内網はプライベートで運用する、というプラクティスが普通なのだから、v6もそうしたい、っていうだけなのですけれどね。。。とおもっていたら。。。

(実は古くて) 新しい提案。ULAをv4より優先に

draft-ietf-6man-rfc6724-update-03

Preference for ULAs over IPv4 addresses in RFC 6724

“ This draft focuses on a specific problem that has arisen involving preference for IPv4 over ULA addresses

Caused by low precedence for fc00::/7

Which means RFC1918 (and all IPv4) is chosen over ULAs

Inconsistent with GUA policy, and suboptimal for **removing IPv4** ”

ま、いろいろといっていますが、ULAをPrivate v4よりも優先するようにしようよ
っていうより、v6全体をv4より優先に。という提案

v6全体をv4より優先に、といわれたので、NATとは関係なくNAT反対派でも反対できない

なんと、IETF Last Callがかかり、RFCとなる道筋がついています。ほどなくRFCとなり、各OSにパッチが
できるはず。。。来年くらいかな?? (Update)

しかし、実際にはこれはNATの導入を加速するはず

デュアルスタック環境で、ULAがPrivate v4あるいはGlobal v4よりも優先されるようになるのであれば、そこにNAT (NAPTv6にしるNPTv6にしる) があると、ULAがつかわれるようになります

すなわちNATがいろいろなところで利用可能になります

となると、DHCPv6 PD Per Host が使えるかどうかとは、独立に、あちこちでNATをつかったソリューションをつくることができるようになりますと予想されます

要するに「v4と同じようにやればいいです」といえるようになる

繰り返しになりますが、私は
v6NATを使えるようにして、v4と同じやり方、も許しつつ、
可能な限り、この新しいPD Per Hostをつかえるところではつかっていく
というのがよいやりかたなのではないでしょうか
とおもっております

NPTv6 で作るほうがNAPTより性能がいいはず

- ほんらい、v6がNAT無しにこだわっているのは、エンドツーエンドでIPSECをつかう。そしてPKIなりなんなりで暗号化をきちんと行う
- ということにこだわってるからなのではないかとおもいます
- しかし、実際には企業網を運用する側から見ると、QUICのように末端で全部暗号化してしまっただけではぜんぜんわからない、というのはセキュリティ保護上、看過しえない、という人たちもいますので、この原則をまもることは結構議論のまともになります
- また、QUICはNAPTのセッション数を使いつぶしてしまうという問題があるわけですが、これに対しては、NPT v6はセッション数制限はありませんのでQUICとの相性もいいので、企業網をULAをPrivateアドレス扱いで設計してNPTv6をつかってミドルボックスで制御を強制する、というモデルは、v4でNAPTをつかうよりはるかによいアイデアだということになります
- **この点からも企業網でもなるべくはやく全面的なv6化をすすめるほうがいい、といえるのではないのでしょうか**

プリンターとかファイルシェアとか

特に企業網の中には外と通信してほしくないものがある

- たとえば、ファイルシェアとか、プリンターとかは、外と通信してほしくない、わけです
- これをv6に無理やりしてしまうのはどうなの？ってことなのですが。。
- というわけで、v6でもプライベートアドレスが欲しいということになる。ULAでいいじゃんってことですけれど。
- V6って複数のアドレスが付いてしまうので、その管理も大変。
- DHCPで管理するやりかたにもっと寄せていくことも必要だと思います
- 実際、企業用のプリンターのv6対応はほとんど後退してしまっています（しらべました）。つかわれなもんね
- ファイルシェアは結構あぶない。無自覚に外に開いているかもしれないのでご注意を。

それでもv6化はすすむ

だんだんコンシューマーがv6化していくので

- そうはいつでも、
- インターネットのコンシューマーの部分がどんどんv6化していってますので
- **わりと早い時期に「企業網からもv6アクセスが必要である」という状態になるんじゃないか**と思います
- **そういうキラーアプリ**がでてくるんじゃないかな、っていうか、でてきたらすぐですね

- **なんかLineとかそういう感じのやつとか。。**わからないですが、**v6じゃないとうごかないんだけど便利っていうツール。**

- **昔、v4を広めていたころに「電子メールなんて企業じゃ使わないよ。FAXだよ」**ってよくいわれてたんですよねえ。。。

先日のInteropのShownet

- 先日行われたInteropでのShownetでは、SR6 (Segment Routing 6) をコアに使い、Link Local アドレスだけでルーター群をつなぎ
- エッジルータからEVPNでスイッチ群をつないでいました
- **2024年も同じコンセプトが踏襲されました (UPDATE)**
- すなわちコアにv6だけのL3ネットワークを使い
- 末端ではEthernetパケットをコアのv6にEthernet—VPN**L3VPN**にのっけてつなげていた
- わけです。これは、まさになるほど、とおもいましたね。
- まさにちょっと先の企業ネットワークの作り方としては新鮮かつ単純で有効なやりかたです
 - さすがNOCチーム。。。やるなとおもいました

SR6にはまだまだ課題（特にセキュリティ面）があるのも事実ですが、面白い動きだと思います

uPNP か、PCPあたり

- 仮にNATをつかうこととなったら
- 議論の分かれるところですが、v4では使われることの多かったuPNPのv6への実装あるいはPort Control ProtocolとしてRFCが決まっている規格の実装をホームゲートウェイとかにするというのも、あらためて検討が必要な気がしています
- NAPTを廃止するので、外部からLANへの疎通が自由になるとスキャンされますので、v6でもあちこちにステートフルファイアウォールを仕込むべきだという意見に私も賛成です
- そうなるとそのステートフルファイアウォールを制御する仕掛けが必要になるということなだけなのですが、うまく標準的なやりかたがきまるといいなとおもいます
- まあ、実はこのあたりは企業網にはあまり関係ないのかもしれませんが。。。

まとめ

- 社内網でつかえるようにするためにはv6にもNAT（ただしたぶんNPTv6。NAPTではなくて）をつかえるようにするといいいとおもいます
- ULA（Unique Local Address）をもっとちゃんと使えるようにしたいのでアドレス選択ルールだけはかえないといけない（でもRFCになればきっとWindows UPDATE などが変わります）
- v6NATを使えるようにして、v4と同じやり方、も許しつつ、
可能な限り、PD Per Hostをつかえるところではつかっていく
というのがよいやりかたなのではないでしょうか
- キラーアプリは突然来るとおもいます。そのときに慌てないように。
- いまでもv6は普通に流れているので「なかったこと」にするのは逆に難しいです
- どうぞ皆さま抜かりなく準備して行ってくださいませ



ご清聴ありがとうございました