Internet Week ショーケース in 広島

世界で進むIPv4の品質劣化とIPv6の導入、ところで企業のIPv6対応は?

2018.5.31

日本インターネットエクスチェンジ㈱

a-nakagawa at jpix dot ad dot jp

中川あきら

会社概要

社名	日本インターネットエクスチェンジ株式会社 (JPIX)
設立	1997年7月10日
資本金	451百万円
株主	• KDDI株式会社 • 株式会社ブロードバンドタワー • ソフトバンク株式会社 • ソニーネットワークコミュニケーションズ株式会社 • ビッグローブ株式会社 • 富士通株式会社 • 株式会社朝日ネット • 株式会社ケイ・オプティコム • 三菱電機インフォメーションネットワーク株式会社

- 日本初商用IX
- ISP等9社出資
- 中立・IX専業

- 顧客数日本最大 約170社
- トラヒック増
- 地方/海外顧客増

自己紹介

- 氏名
  - 中川あきら
- 所属
  - 2010年4月～ 2017年3月　JPIXとJPNEを兼務
  - 2017年4月～　JPIX
- 本日の講演に関する主な活動
  - RFC6888 CGN　Co-author
  - Internet Week 2017　プログラム委員(IPv6担当)
  - IPv6 Summit 運営　インターネット協会
  - JPOPF 運営　JPOPF運営チーム(旧ポリシーWG)
    (JPOPF Steering Team : JPOPF-ST)

広島とわたし

- 2009年
  - IPv6セミナー (1回目)
  - IETF76実行委員で広島に何度も通う。

<期間が空く>

- 2017
  - IPv6セミナー (2回目)
- 2018
  - IPv6セミナー (3回目)
  - JANOG41
  - IWショーケース(本日)

Internet Week 2017 での試み

「法人」のIPv6を採り入れました。

- IPv6を導入している企業は極めて少ない。
- 業界にノウハウが乏しい。
- 興味を持つ人は少ない。
- しかし、少しでもきっかけが必要。

→ 集客できなくても良い。やるべきだ !!

IW2017 IPv6セッション登壇者

※ 本日の資料の構成順

IPv6の普及状況
中川 あきら(日本インターネットエクスチェンジ株式会社(JPIX))

IPv6の普及状況とセキュリティ対策の必要性
IPv6セキュリティ概説-運用編-
藤崎 智宏さん (日本電信電話株式会社)

IPv6セキュリティ概説-プロトコル編-
北口 善明さん (東京工業大学 学術国際情報センター)

企業ネットワークのIPv6対応
廣海 緑里さん (株式会社インテック)

本セッションについて

Internet Week 2017におけるIPv6関連の各発表を忠実に再現するものではありません。

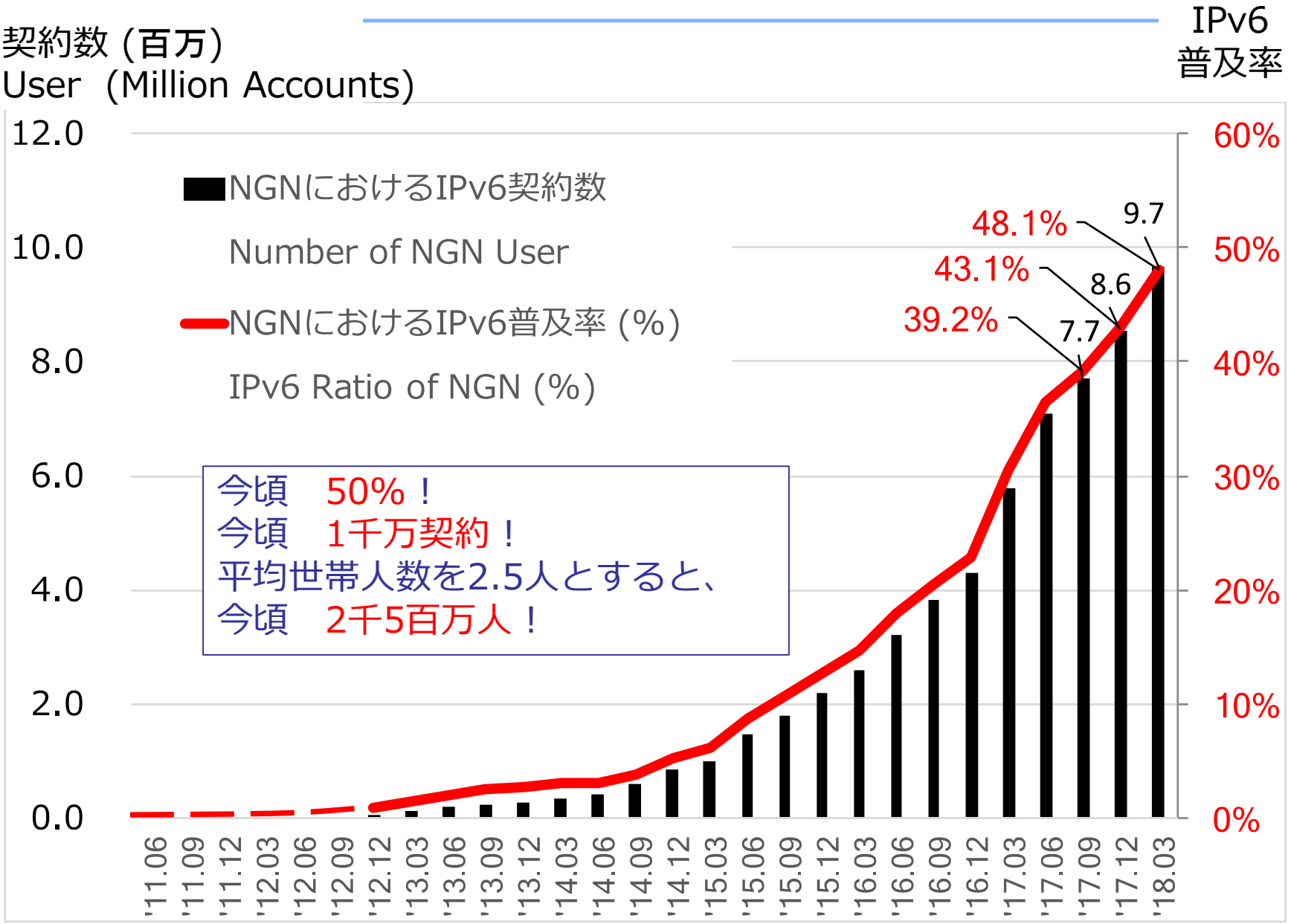
各発表内容を自分の言葉に置き換え、アレンジしました。

講師の資料を切り貼りしたスライドも存在しますが、その際には出典 URL を記載しました。

目次

- **IPv6普及状況**
- IPv6のセキュリティー
- 法人のIPv6

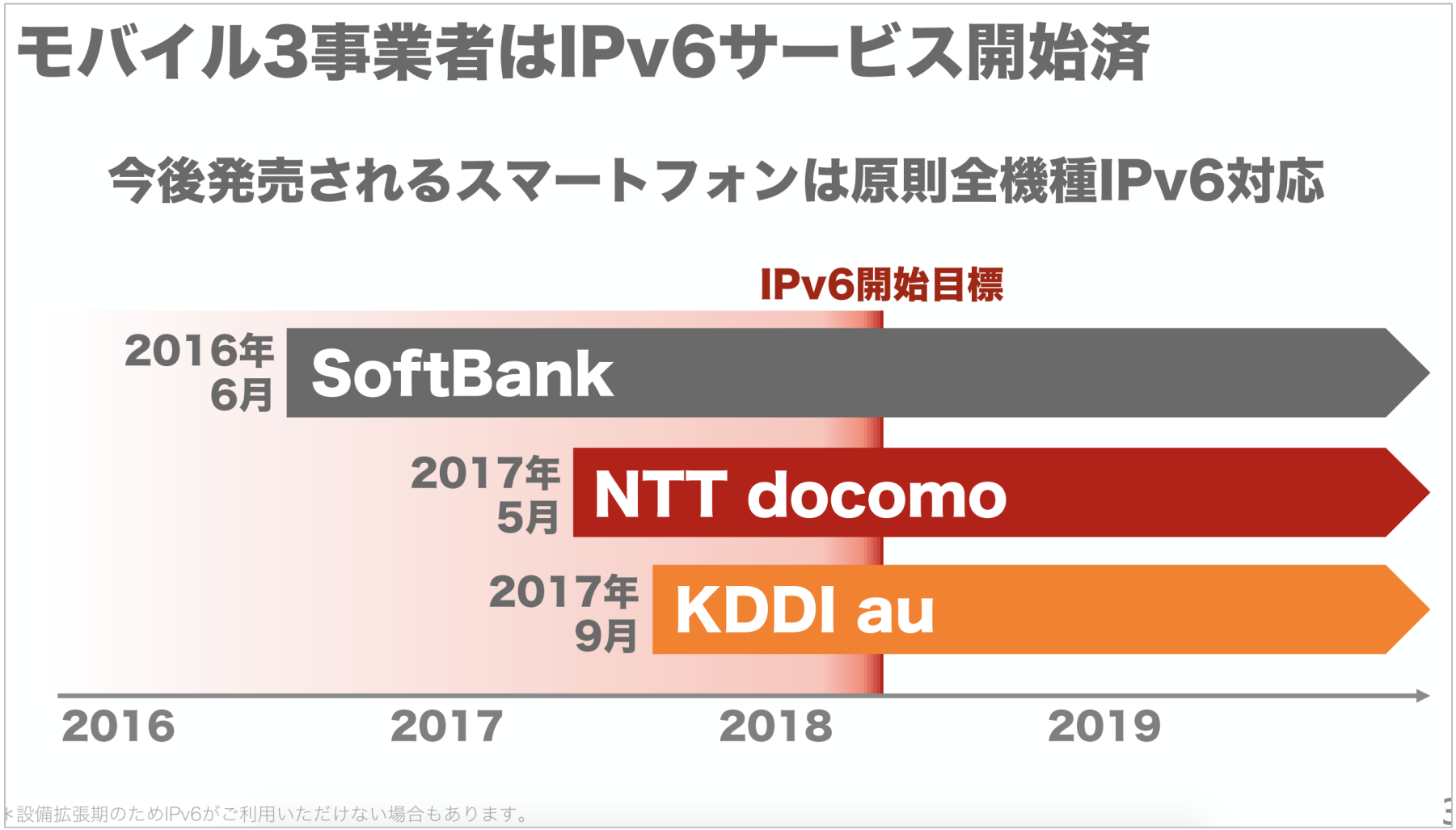
国内で進むIPv6・NGNにおけるIPv6対応状況



IPv6 高度推進・普及委員会
http://v6pc.jp/jp/spread/ipv6spread_03.phtml

国内で進むIPv6・モバイル3社

本格対応開始 !!



Source：総務省
http://www.soumu.go.jp/main_content/000517037.pdf

国内で進むIPv6・CATVの IPv6

「ドコモ光 タイプC」のサービス提供がIPv6対応の新しいモチベーションとなっている。

「ドコモ光 タイプC」とは、 ケーブルテレビの設備を使ってドコモが提供する光インターネットサービス(卸サービス)

CATV事業者がドコモにサービスを卸す際にIPv6対応が条件となっている。

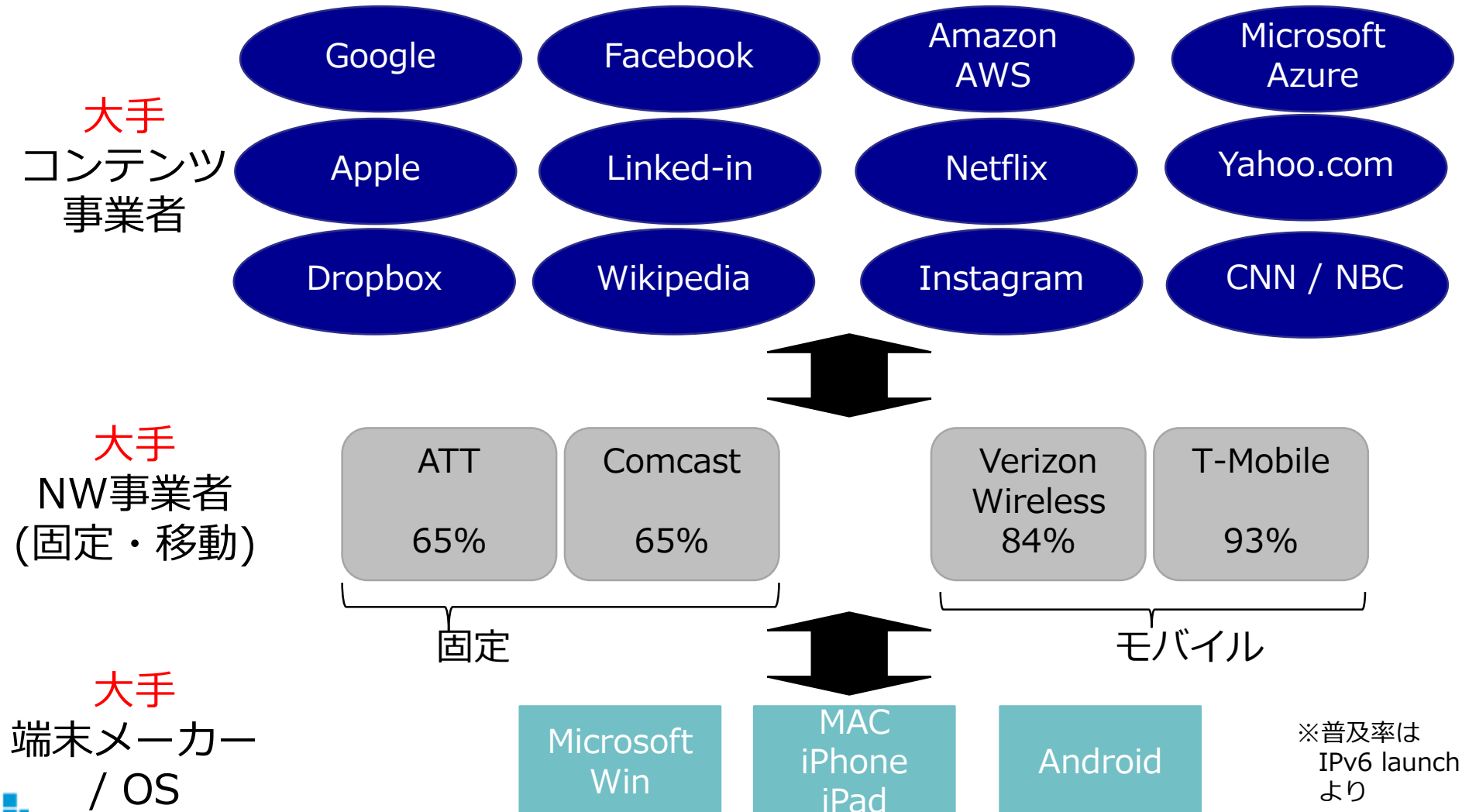
	提供エリア※
株式会社シー・ティー・ワイ	三重県四日市市、いなべ市、桑名市（長島町のみ）、菰野町、木曽岬町
株式会社ケーブルネット鈴鹿	三重県鈴鹿市
近鉄ケーブルネットワーク株式会社	奈良県奈良市（旧月ヶ瀬村、旧都祁村は除く）、生駒市、天理市、生駒郡、香芝市、大和郡山市、大和高田市、葛城市、桜井市、北葛城郡、橿原市、磯城郡、高市郡、御所市、五條市（旧西吉野村、旧大塔村は除く）、大阪府四條畷市（一部のみ）
株式会社 エヌ・シィ・ティ	新潟県長岡市、三条市、見附市
株式会社 ニューメディア	北海道函館市、七飯町、北斗市、山形県米沢市、南陽市、高畠町、川西町、福島県福島市、新潟県新潟市
株式会社 テレビ小松	石川県小松市、能美市

増加中

Source : ドコモ
https://www.nttdocomo.co.jp/hikari/charge/type_c/

USの主要プレーヤーのIPv6対応状況

各プレーヤーが、すさまじいスピードでIPv6対応中。
→ 多くのプレーヤーは世界進出しているため各国でもこの傾向！



※普及率は
IPv6 launch
より

クラウドのIPv6対応 (Facebook社)

Legacy support on IPv6-only infra

Glenn Rivkees

2017年1月18日

Over the past few years, Facebook has been **transitioning its data center infrastructure from IPv4 to IPv6**. We began by dual-stacking our internal network — adding IPv6 to all IPv4 infrastructure — and decided that all new data center clusters would be brought online as IPv6-only. We then worked on moving all applications and services running in our data centers to use and support IPv6. Today, 99
We anticipate moving ou
few years.

- Facebook Data Center(DC)内
  - Dual Stack から IPv6-onlyへ
  - 全アプリとサービスをIPv6対応へ
  - 現在、DC内部の99%はIPv6、内半分はIPv6-only
  - 数年後に IPv4 廃止へ
- Internet からのアクセス
  - 15%がIPv6・85%がIPv4
  - IPv4アクセスは Load Balancer で IPv6に。

Wow !!

Source: Facebook https://code.facebook.com/posts/635645183305089/legacy-support-on-ipv6-only-infra/

IAB(*1)の声明 (← ≒ IETF)

IAB は、標準化団体のIETFにおいて今後の新しいプロトコルではIPv4への後方互換を廃止し、IPv6で最適化するよう期待。

← Please comment on IAOC candidates for IAB selection

IAB report to the community before IETF 97 →

IAB Statement on IPv6

Posted on 2016-11-07
by Cindy Morgan

The Internet Architecture Board (IAB), following discussions i
Development Organizations (SDOs) and organizations that th
seeing an increase in both dual-stack (that is, both IPv4 and
networking standards need to fully support IPv6. The IETF as

The IAB expects that the IETF will stop requiring IPv4 compa
and depend on IPv6.

Preparation for this transition requires ensuring that many dif
dependent on IPv4 [see RFC 6540]. We recommend that all
IPv4. We recommend that existing standards be reviewed to
IPv4, via dual-stack or a transition technology, will be needed
standards which prevent or slow down the transition in differe

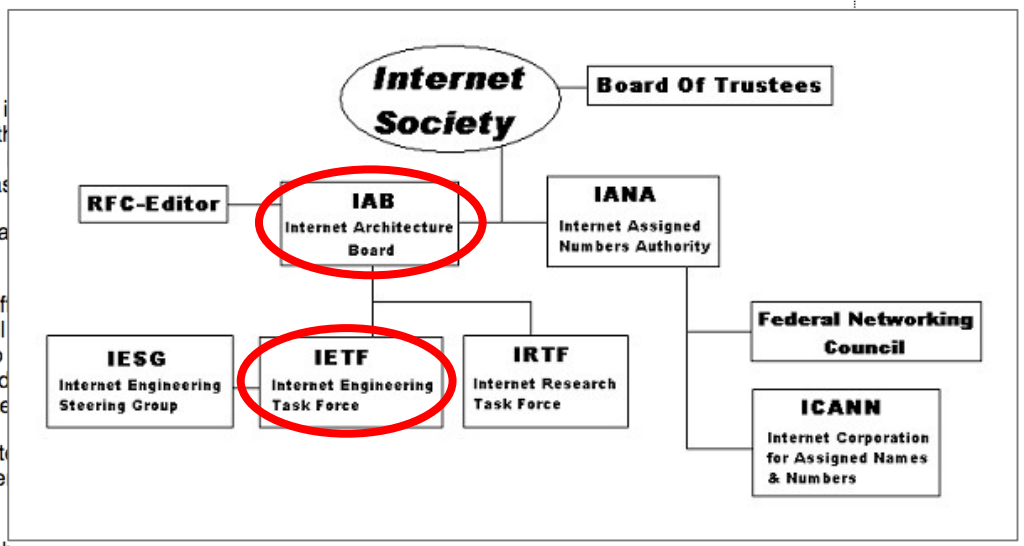
In addition, the IETF has found it useful to add IPv6 to its ext
since this helps our participants and contributors and also se
to other SDOs.

We encourage the industry to develop strategies for IPv6-only
further developments in IPv6 or other protocols. We are also

This entry was posted
in Announcements,
IAB Statements.
Bookmark the
permalink.

← Please comment on IAOC candidates for IAB selection

Comments are closed.



Source：
https://de.wikipedia.org/wiki/Internet_Society

(*1) IAB：インターネットの技術コミュニティ全体の方向性やインターネット全体のアーキテクチャについての議論を行う技術者の集団。

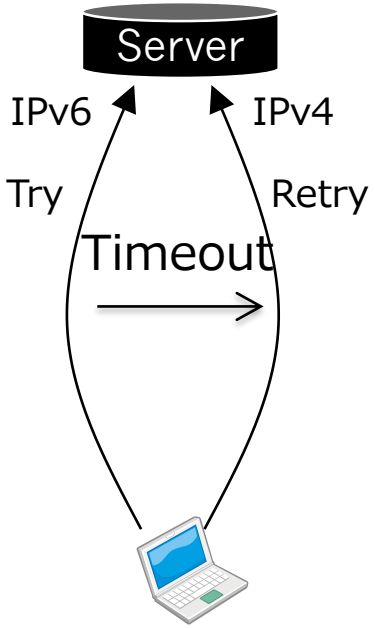
Source：https://www.iab.org/2016/11/07/iab-statement-on-ipv6/

IPv6 優先に関する標準化

New

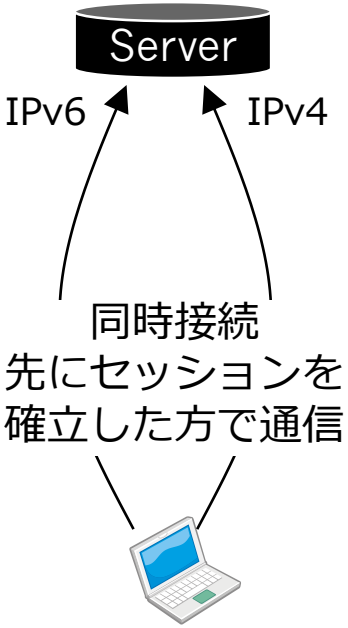
Happy Eyeballs v2 (RFC8305) により、IPv6・IPv4の両接続がある場合、IPv6を優先

Fallback



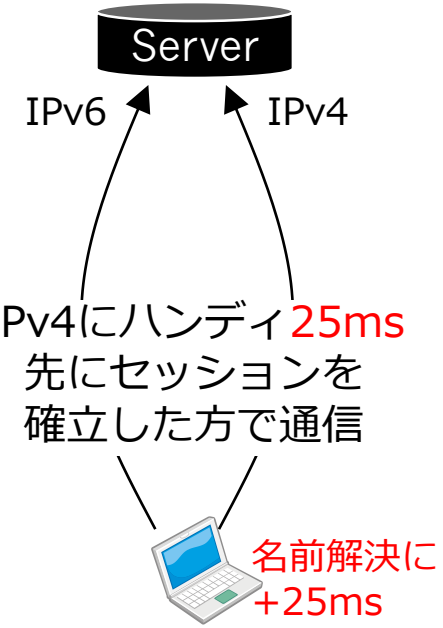
IPv4での接続時にTimeoutを待つ必要があった。

Happy Eyeballs (RFC6555 2012)



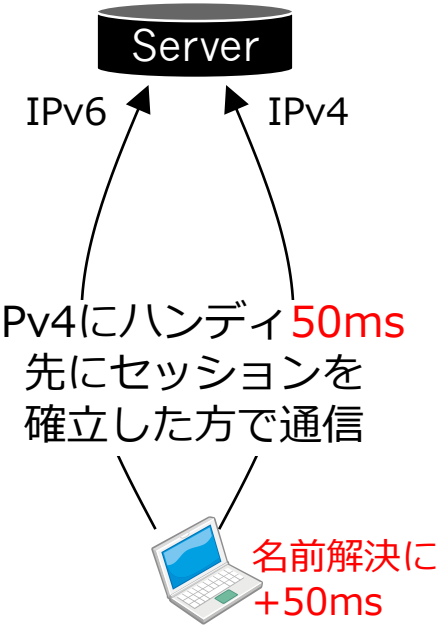
改善

Happy Eyeballs (Apple独自仕様 2015)



意図的にIPv4に+25ms

Happy Eyeballs v2 (RFC8305 2017.12)

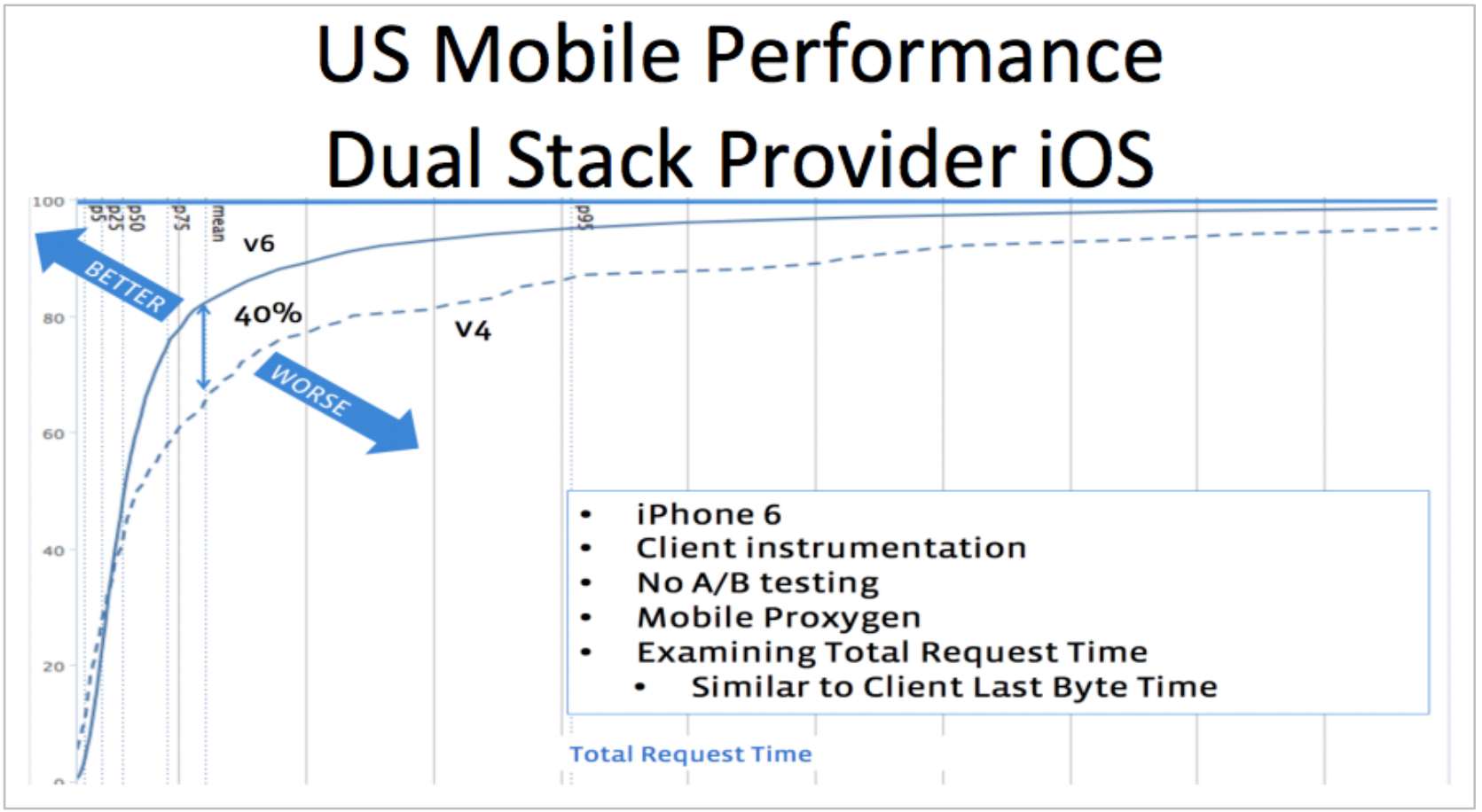


+50msへ

- Clientは ”Resolution Delay” を待つこと (Should)
- Resolution Delayは 50ms (Recommended)

IPv4の現状：速度が極めて遅い例

アメリカにおけるモバイル商用回線のIPv4のパフォーマンスの悪さを指摘。(Facebook社プレゼンより)

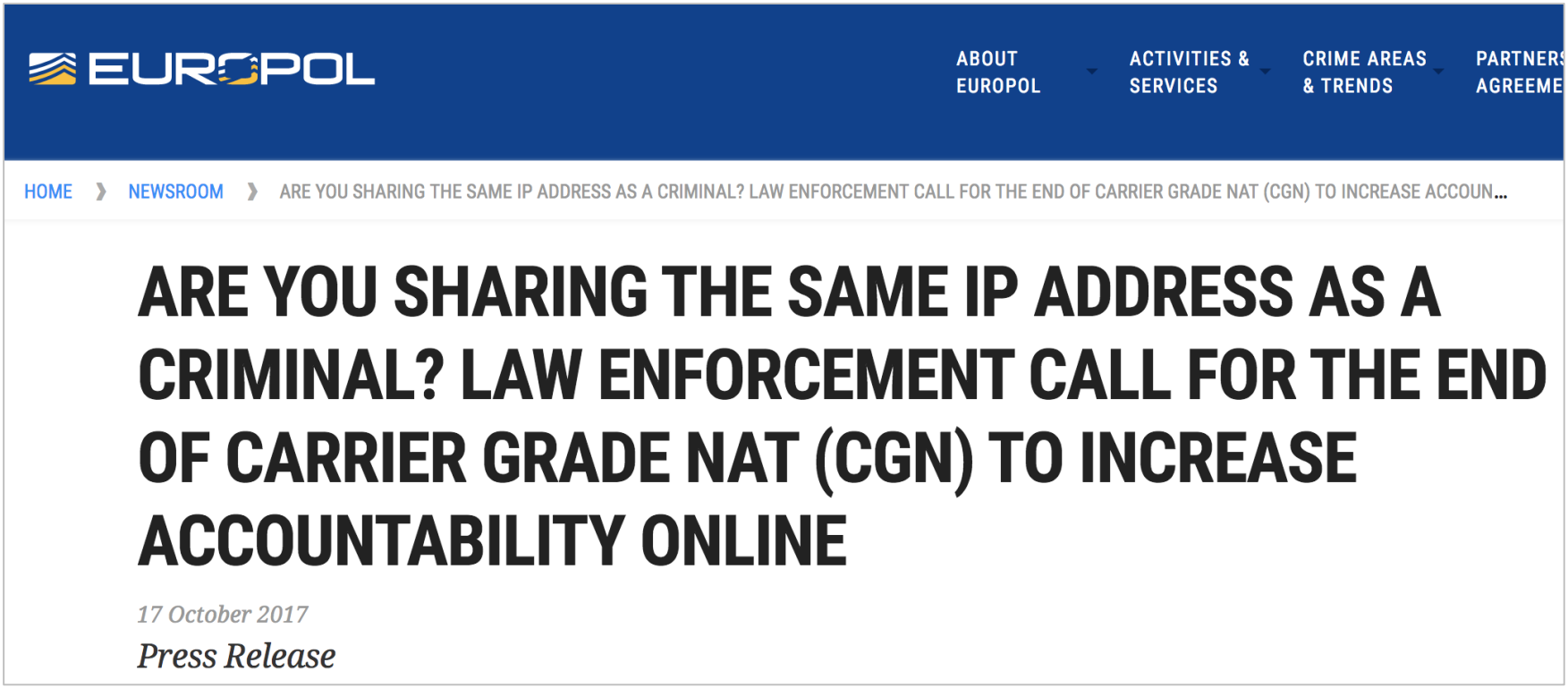


Source：NANOG64
https://www.nanog.org/sites/default/files//meetings/NANOG64/1033/20150602_Huston_The_Benefits_Of_v3.pdf

IPv4の現状:アドレス共有に関連する問題提起

Europolより、
CGN配下の「犯人を特定できない」といった問題提起が出ている !!

Europol : 欧州刑事警察機構

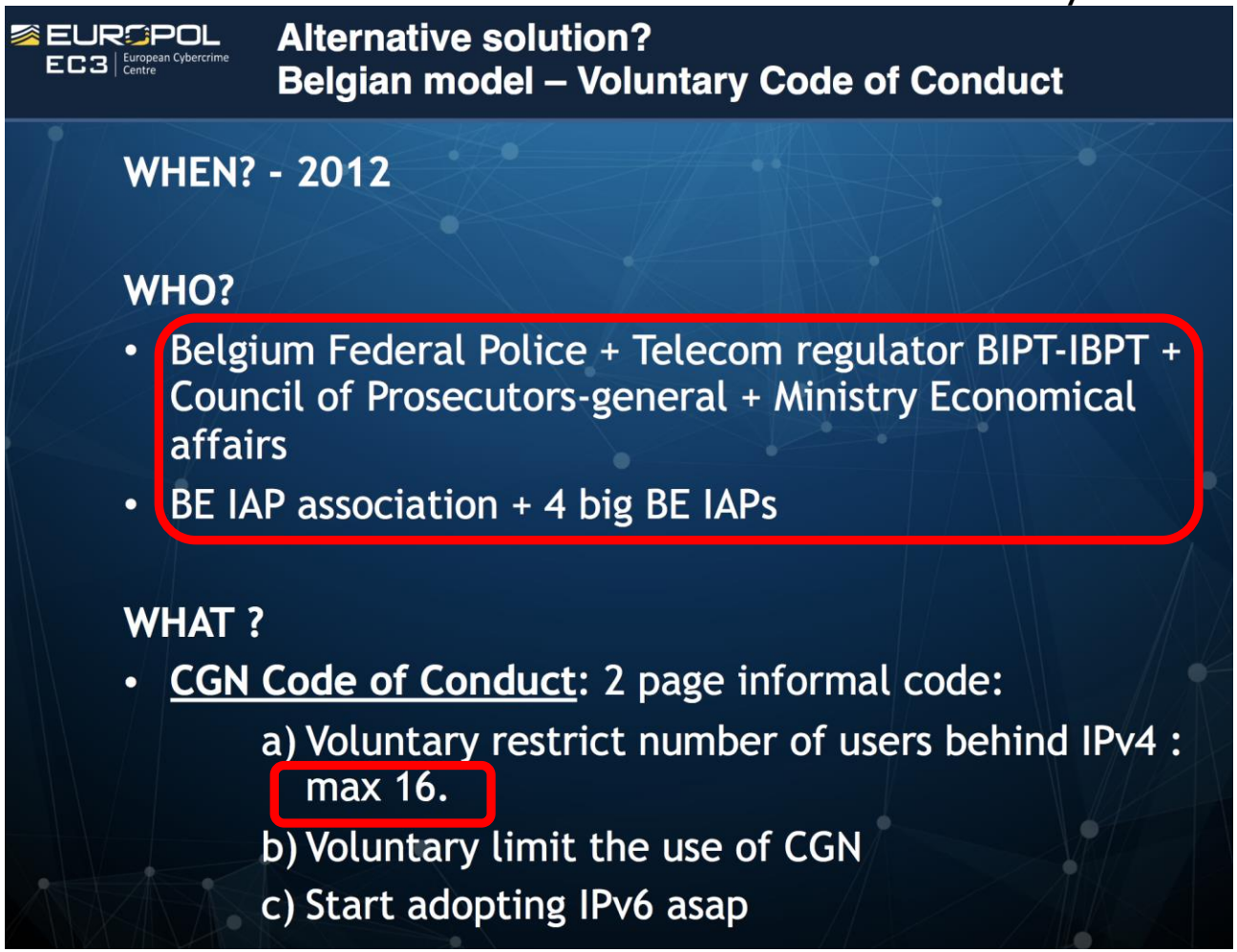


https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online

ベルギーの事例：IPv4 1個当たりの最大共有数

警察を含む各組織で、最大16加入者としている。

May.2017



IAP: Internet Access Provider

Source: https://ripe74.ripe.net/presentations/125-CGN-presentation-Greg-Mounier-EC3-RIPE-74-Budapest.pdf

国内大手事業者の事情・PPPoE方式の現状 ＝ 輻輳

2017年1月、総務省のパブコメにおいて、個人・企業・業界団体等の多くが PPPoE方式の網終端装置における輻輳(混雑)について指摘。

別紙１

次世代ネットワーク（ＮＧＮ）等の接続ルールに関する意見提出者の一覧

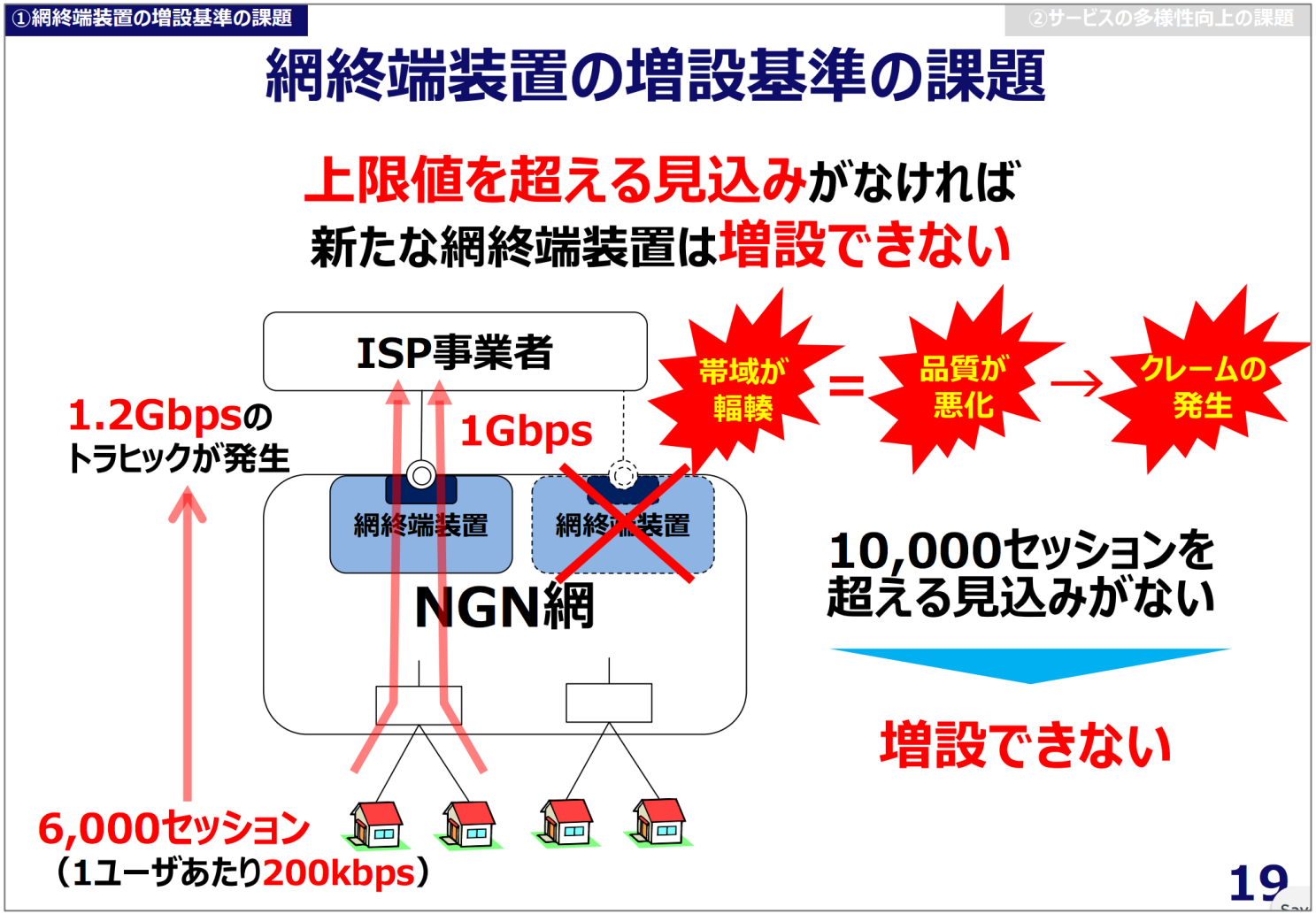
（受付順、敬称略）

意見提出者（計 18 件）				
受付	意見受付日	意見提出者	代表者氏名等	
1	平成 29 年1月 31 日	個人	－	－
2	平成 29 年1月 31 日	個人	－	－

Source：http://www.soumu.go.jp/main_content/000467068.pdf

PPPoE方式輻輳の理由

網終端装置の増設基準が「セッション数」であるため。
トラフィックが増えてもISPの判断で増設できない。

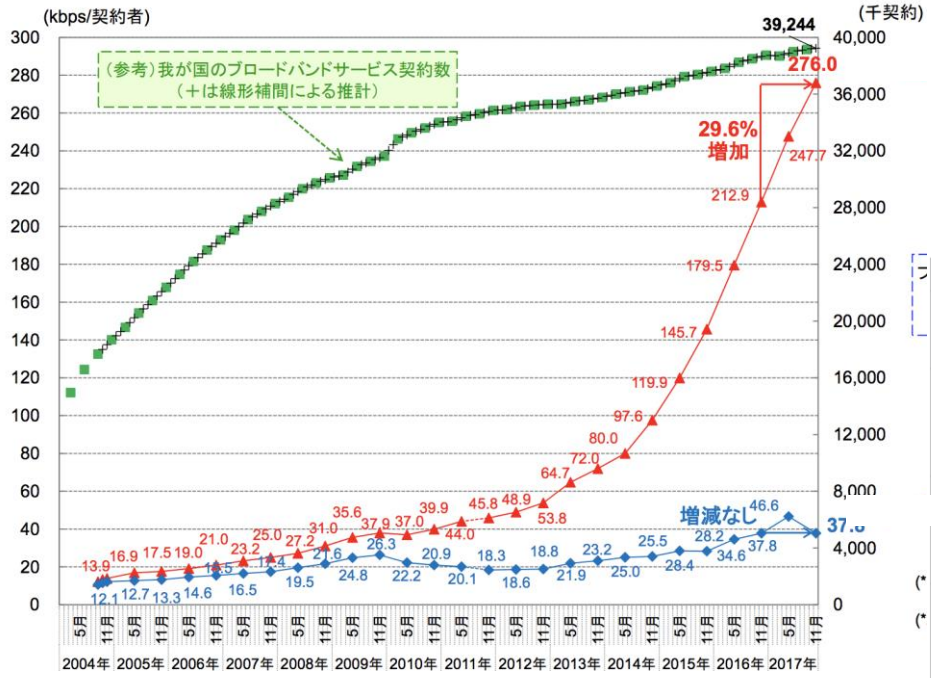


Source：http://www.soumu.go.jp/main_content/000478903.pdf

PPPoEの輻輳度合い

年々、PPPoE(≒IPv4)の輻輳は悪化している。
帯域は一定、1契約当たりのトラフィックは年々増加中。

総務省算出の1契約当たりのトラヒック
2017年11月：276kbps



http://www.soumu.go.jp/main_content/000535404.pdf

(参考)
NTT東西社の増設基準は
中型網終端装置の場合、IPv4・IPv6
それぞれ、
1Gbps IFに8,000セッション
→ 130kbps / セッション(換算)

提供開始時期	2011年度以前	2011年度	2013年度	
提供メニュー（NTT東日本の例）	小型NTE	大型NTE	中型NTE	増設基準を緩和したメニュー
①ＩＦ帯域	100Mbps /200Mbps	1Gbps	1Gbps	1Gbps
②増設基準セッション数	1,000	10,000	8,000	5,000 / 2,000
③セッションあたり帯域（①÷②）	100kbps	100kbps	130kbps	200kbps / 500kbps

http://www.soumu.go.jp/main_content/000478907.pdf

アドレス共有によるIPv4の劣化 (一つのシナリオ)

各国のJSPによるIPv4アドレス共有によって、エンド端末やアプリで
3つの注意が必要。(主として海外では大きな影響が出るのではないか)

初期 (イマココ)
アドレス共有装置導入

⇓

①アドレス共有そのもの
による影響

中期
詰め込む(*1)

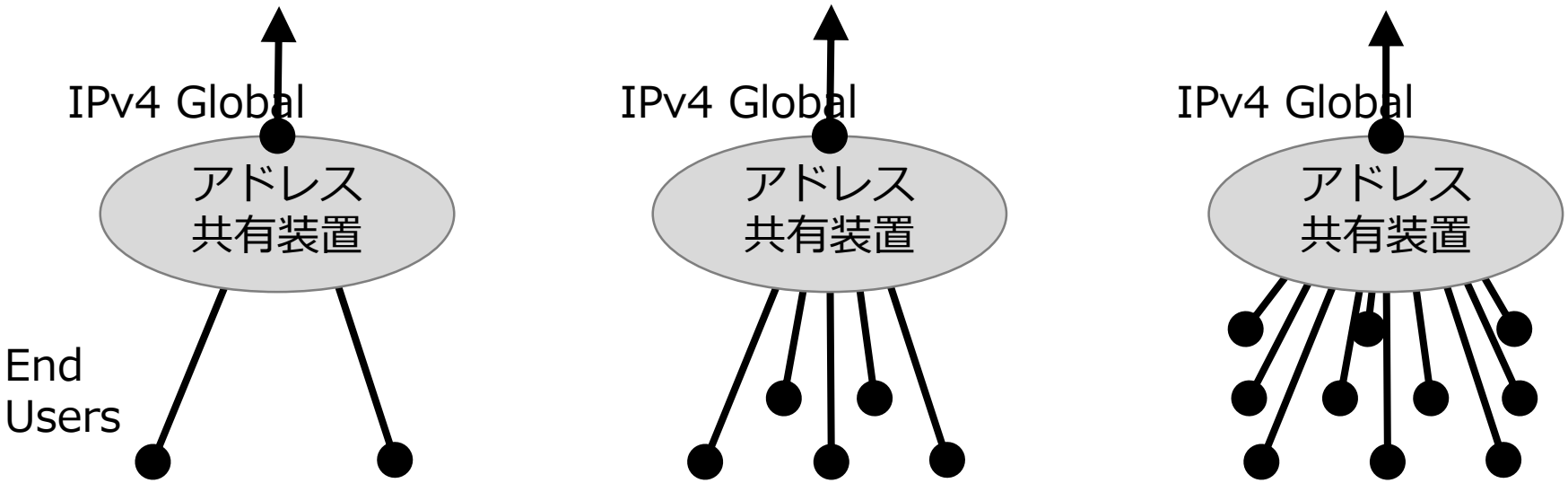
⇓

②ポート番号不足による
影響

末期
NATタイマーを短くし(*1)
ポート番号を確保

⇓

③短時間でのセッション
切断による影響



(*1) MAP-E/MAP-T等のStateless方式の場合は、最初からある一定数のポート数が確保されているため、この影響は出ない。

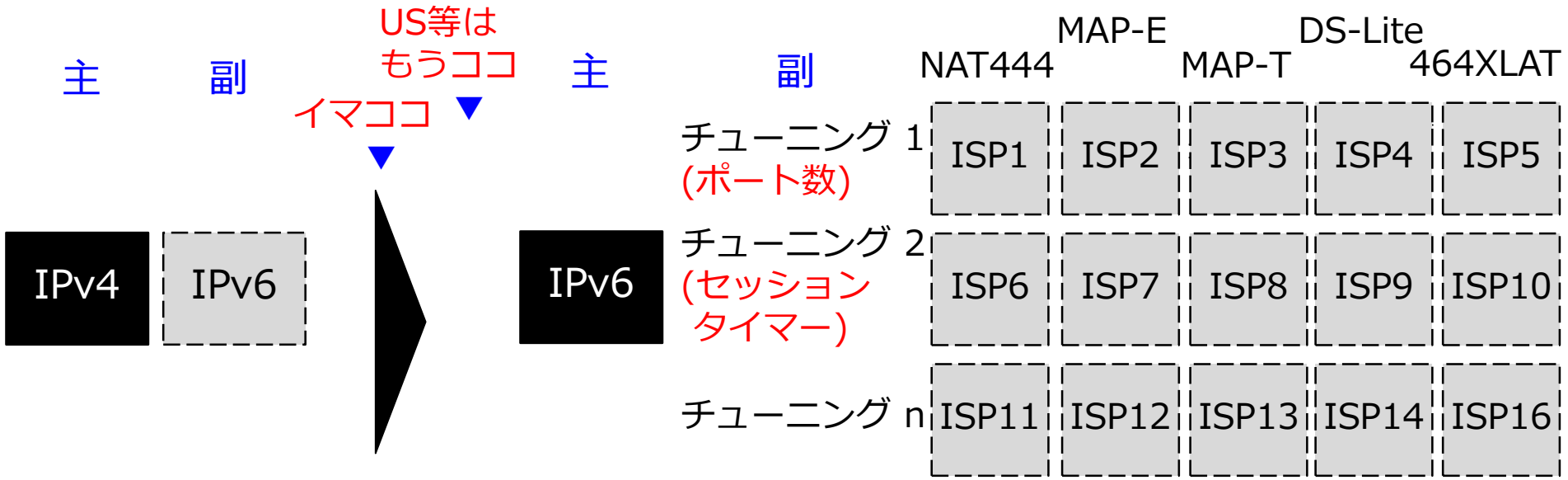
クラウド事業者や端末メーカー・SE等から見たIPv4

世界に市場を持つクラウド事業者や端末/OSメーカー等は、以下を実行中。

- IPv4通信できるようにクラウドや製品等をチューニング
- デグレしないIPv6へのドライブ

IPv6は
追加コストだった。

複数種類のIPv4への対応は
追加コスト



国内のIPv6普及で悩ましいこと

国内での IPv4 の質が秀逸であるために、日本人が世界的な IPv4 のデグレやIPv4離れに気付きにくいこと。

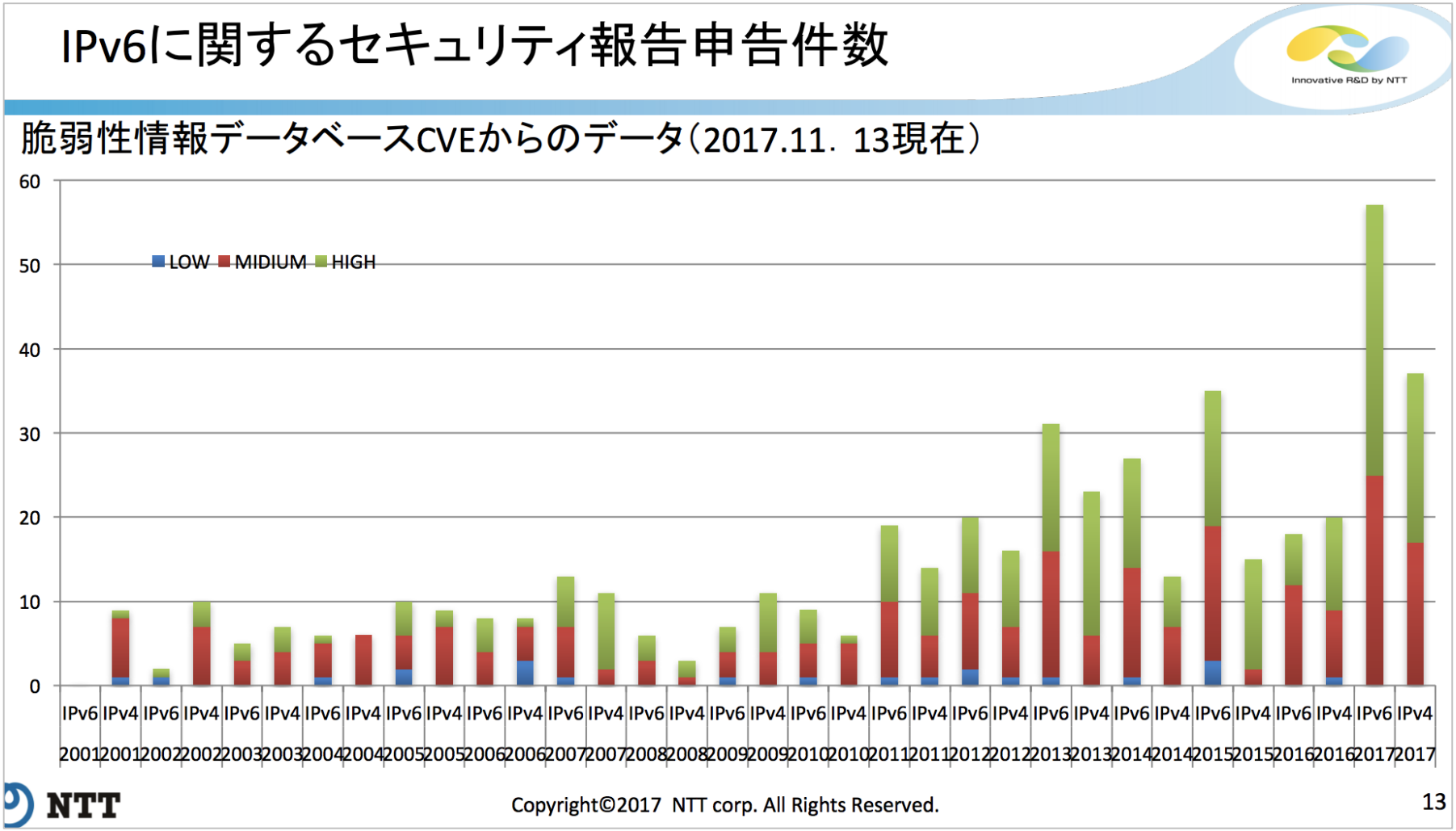
- IPv4アドレスの購入により従来の品質を維持
- IPv4-only機器にも投資
- IPv4 over IPv6 の高い品質
  - 十分な帯域確保
  - 十分なポート数確保
  - NATにおける十分なセッション保持時間確保

国内コンテンツ事業者は
フレッツPPPoE(IPv4)利用者から「遅い」と苦情を受け、
IPv4に懸念を持ち始めた。(イマココ)

目次

- IPv6普及状況
- **IPv6のセキュリティー**
- 法人のIPv6

IPv6に関するセキュリティ報告申告件数



https://www.nic.ad.jp/ja/materials/iw/2017/proceedings/s03/s3-fujisaki.pdf

IPv6セキュリティ対策の必要性

IPv6セキュリティ対策の必要性

Innovative R&D by NTT

- 機器はIPv6対応済み
  - 機器は，ユーザ・管理者が知らないうちにIPv6で通信している
    - リンクローカルアドレスは自動的に付与

IPv6を導入していなくても，IPv6を意識したセキュリティ管理が必要

  - IPv6が広く利用されるようになって来た

多くのセキュリティ報告が上がっており，IPv4と同等の対応が必要

Windows XPの例

NTT

https://www.nic.ad.jp/ja/materials/iw/2017/proceedings/s03/s3-fujisaki.pdf

IPv6におけるセキュリティ

IPv6におけるセキュリティ

Innovative R&D by NTT

- ”IPv6だから”ということはない.
  - 守るべきポイントや，考え方などは基本，”IPv4”と同等
  - 特に，「セキュリティポリシ」は，IPv4とIPv6で同一にすべき

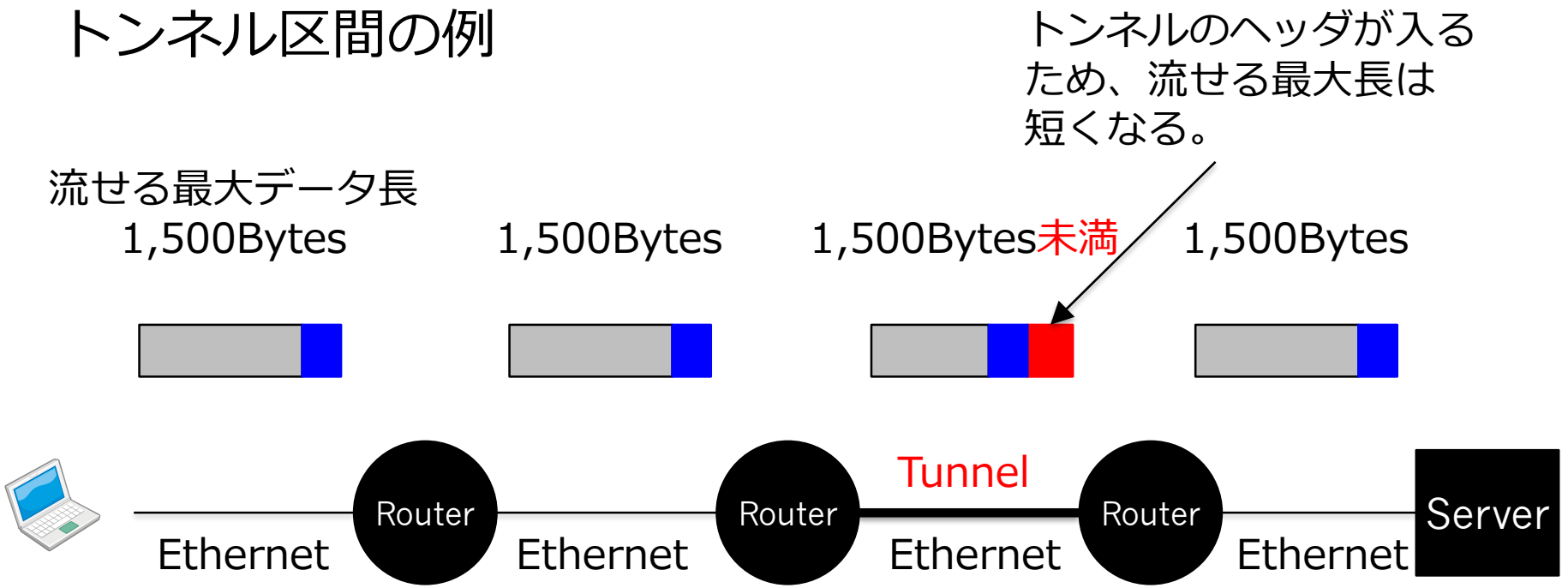
NTT

https://www.nic.ad.jp/ja/materials/iw/2017/proceedings/s03/s3-fujisaki.pdf

技術的背景

インターネットの通信において、長いパケットが通らない場所が存在することがある。

トンネル区間の例

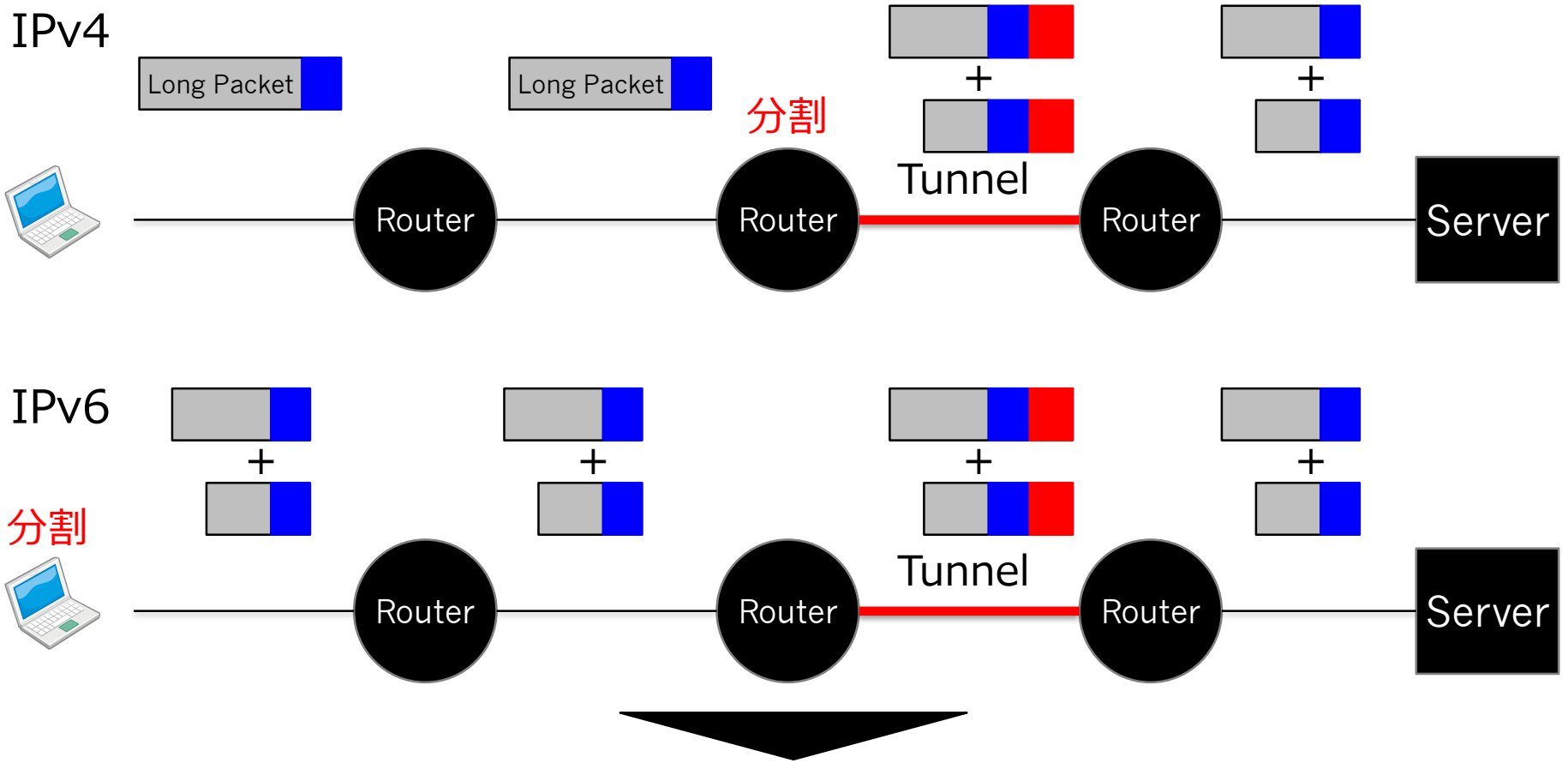


ここで言うトンネルとは、 PPPoE ・ IPv4 over IPv6 ・ IPv6 over IPv4 など。
流せる最大データ長 = MTU (Maximum Transmission Unit)

(Path MTU Discovery)

長いパケットを通す手段、IPv4 vs IPv6

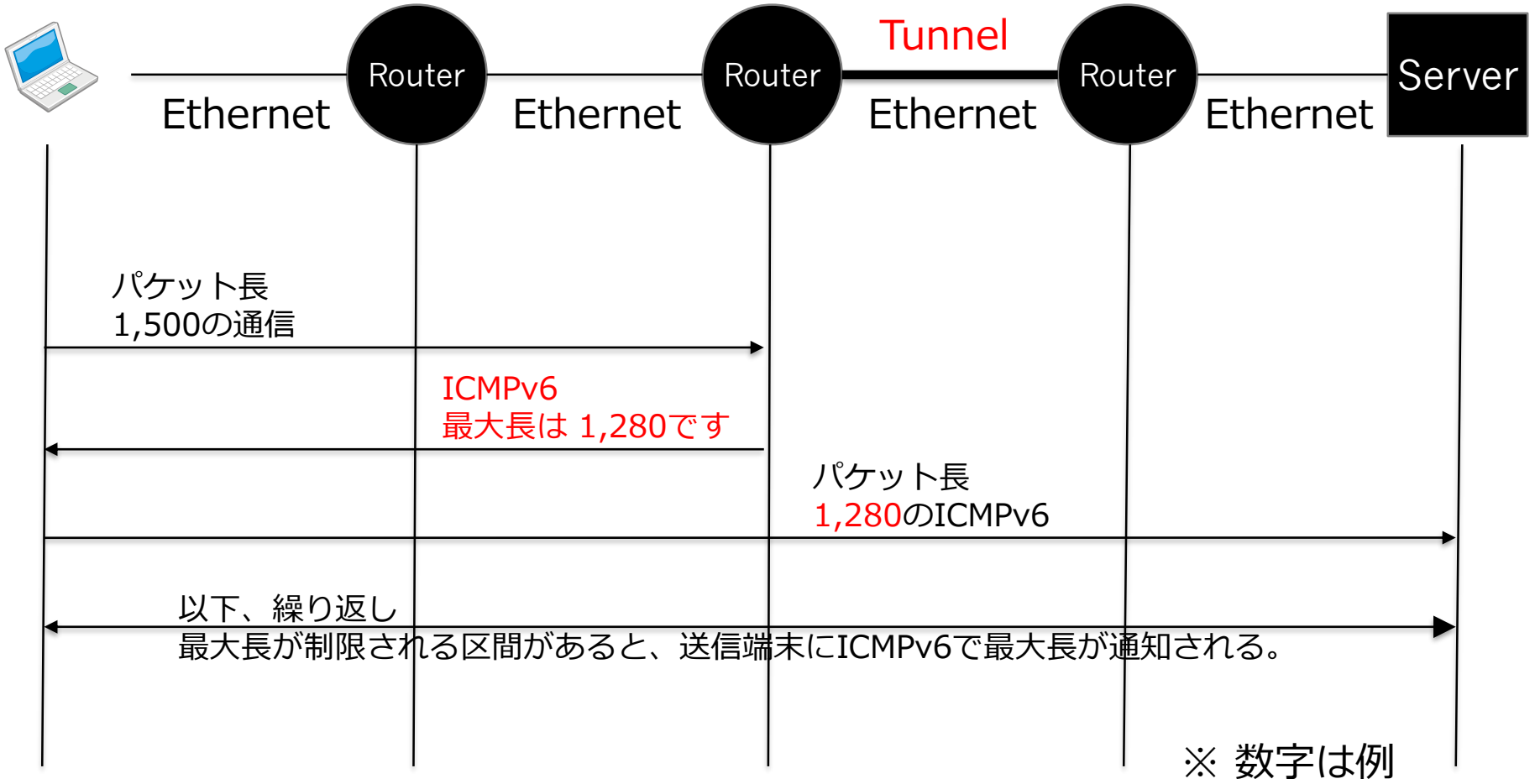
IPv4では、中継ルーターがパケットを分割(フラグメンテーション)していた。
IPv6では、送信端末が分割して送る。



なぜ、送信端末は流せるパケットの最大長を知っている？

送信端末が流せるパケットの最大長を知っている理由

ICMPv6 を使って流せる長さが送信端末に通知される。
この調査の仕組みを Path MTU Discovery という。



(Path MTU Discovery)

Path MTU とセキュリティーの関係は？

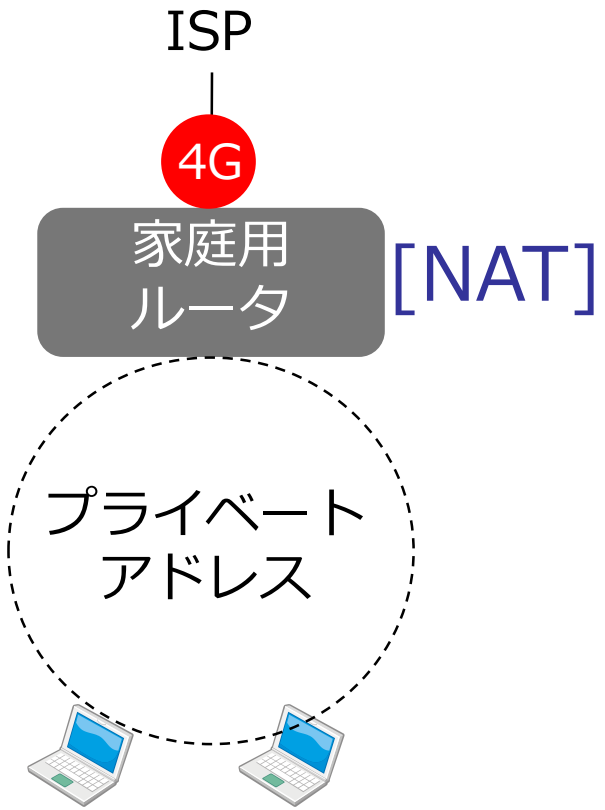
仮に、セキュリティー面で ICMPv6 をフィルターするべき、
という方針があったとしても、
全てのICMPv6をフィルターアウトするべきではない。

IPv4と違い、主信号に影響が出ることがあるため。

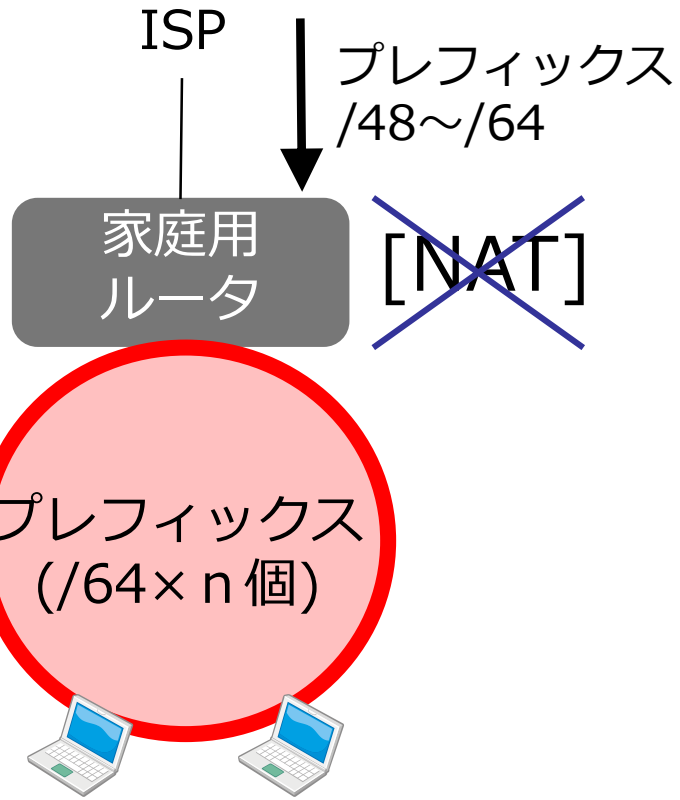
IPv4とIPv6のアドレス払い出しの考え方

ISPが払い出すアドレスの場所とアドレスの種類が異なる。

(IPv4)
家庭用ルータのWAN側
(ISPに隣接するインタフェース)
アドレスを１つ

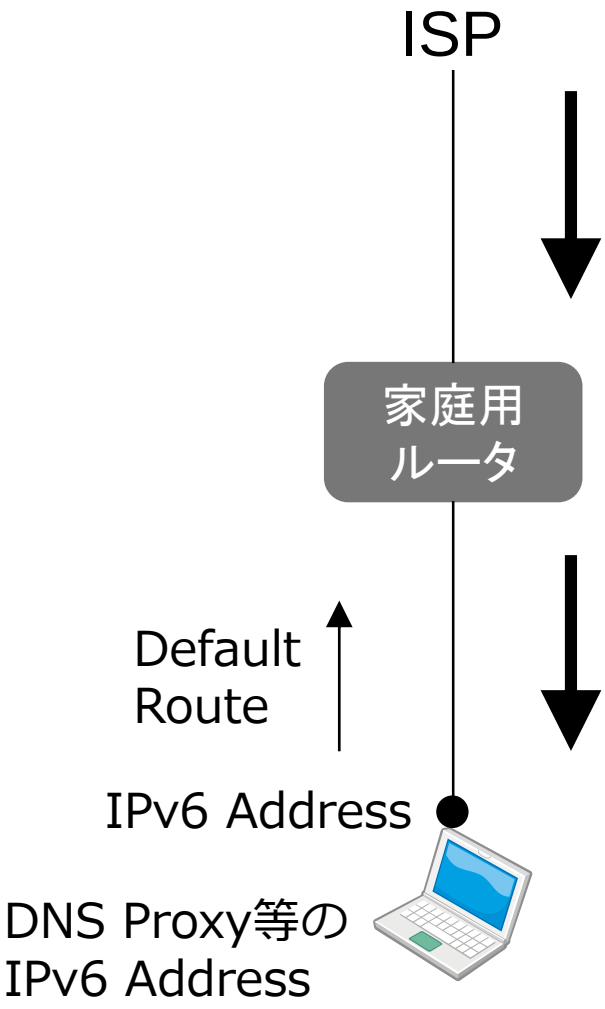


(IPv6)
家庭用ルータのLAN側
(ISPから見ると1ホップ先)
プレフィックス(アドレス群)



アドレス等自動設定のためのプロトコル

多くの場合、端末に各種の情報を自動設定するために複数のプロトコルが併用されている。以下は典型的な例



DHCPv6-PD　(/48・/56等)
(PD：Prefix Delegation)

(例) 2001:0db8:1234::/48

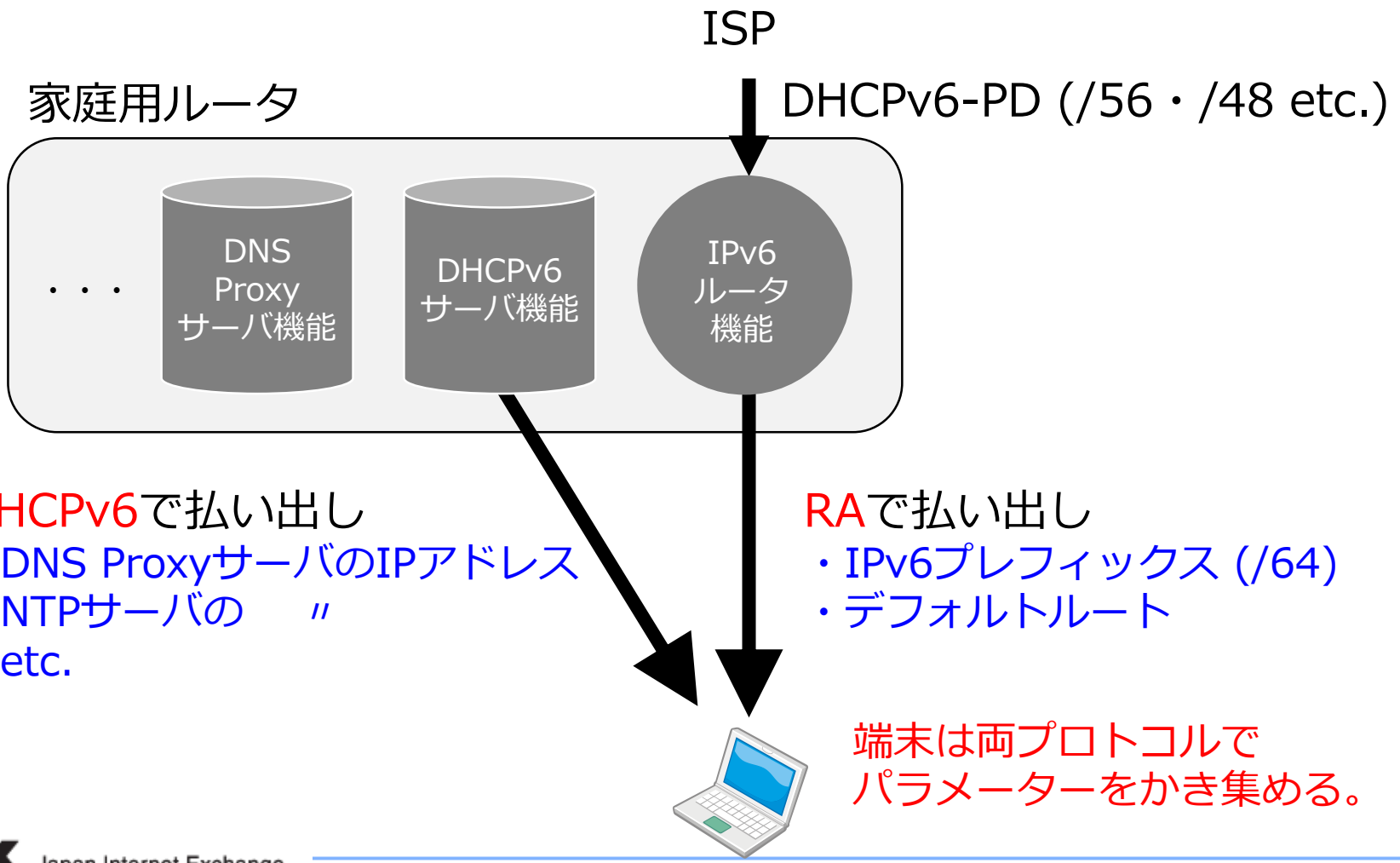
SLAAC方式(*1)
・RA　　(/64のPrefix・Default)
・DHCPv6　(DNSのIP 等)
を併用して自動設定

(例) 2001:0db8:1234:5678::/64

(*1) SLAAC：　Stateless Address Auto Configuration

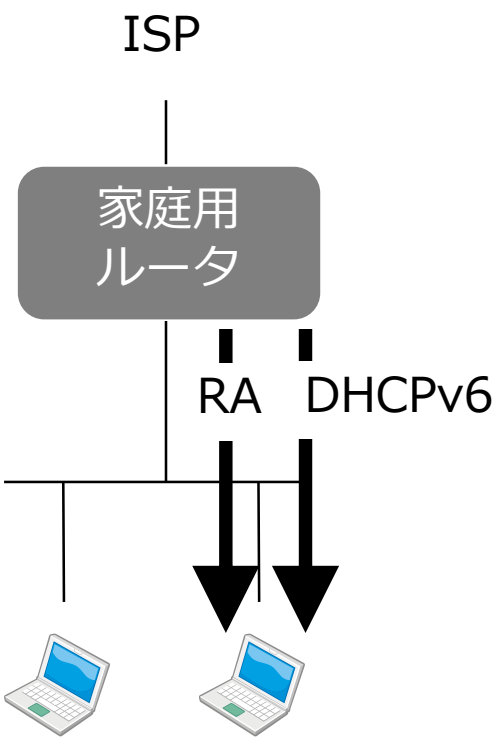
宅内アドレス等の設定動作例 (SLAACの例)

RA　　：プレフィックス(IPアドレス)・デフォルトルート
DHCPv6：DNS ProxyのIPアドレス等 を設定



RA と DHCPv6 で払い出せる情報

多くの端末は RAとDHCPv6を併用してIP Address等の情報を自動設定している。



	RAの機能	DHCPv6の機能
プレフィックス	○ (端末がアドレスを自動生成)	×
アドレス	×	○
デフォルト経路	○	×
DNSサーバのアドレス	△(*1) (RFC5006 後追いで標準化)	○
各種サーバのアドレス (RDNSS, etc.)	△(*1) (RFC6106・8106 後追いで標準化 (*1))	○
特記事項	市場に出回っている製品の全てが(*1)に対応しているわけではないため△。	デフォルト経路を払い出せないため、RAとの併用が前提

IP Address等自動設定のシーケンスイメージ (SLAACの例)

家庭用ルータ

NS：Neighbor Solicitation
IP(LLA(*1)) と MAC は？

NA：Neighbor Advertisement
IP(LLA(*1)) と MAC は、これ。

RS：Router Solicitation
だれかルーターの人いる？

RA：Router Advertisement
私ルーター。IP(GUA(*2))とDefault GWはRAから、DNSのアドレスはDHCPv6から入手せよ。
Prefix と Default GWはこれ。

Request
DNSのアドレスは？

DNSサーバのIPアドレスは、これ。

主信号の通信

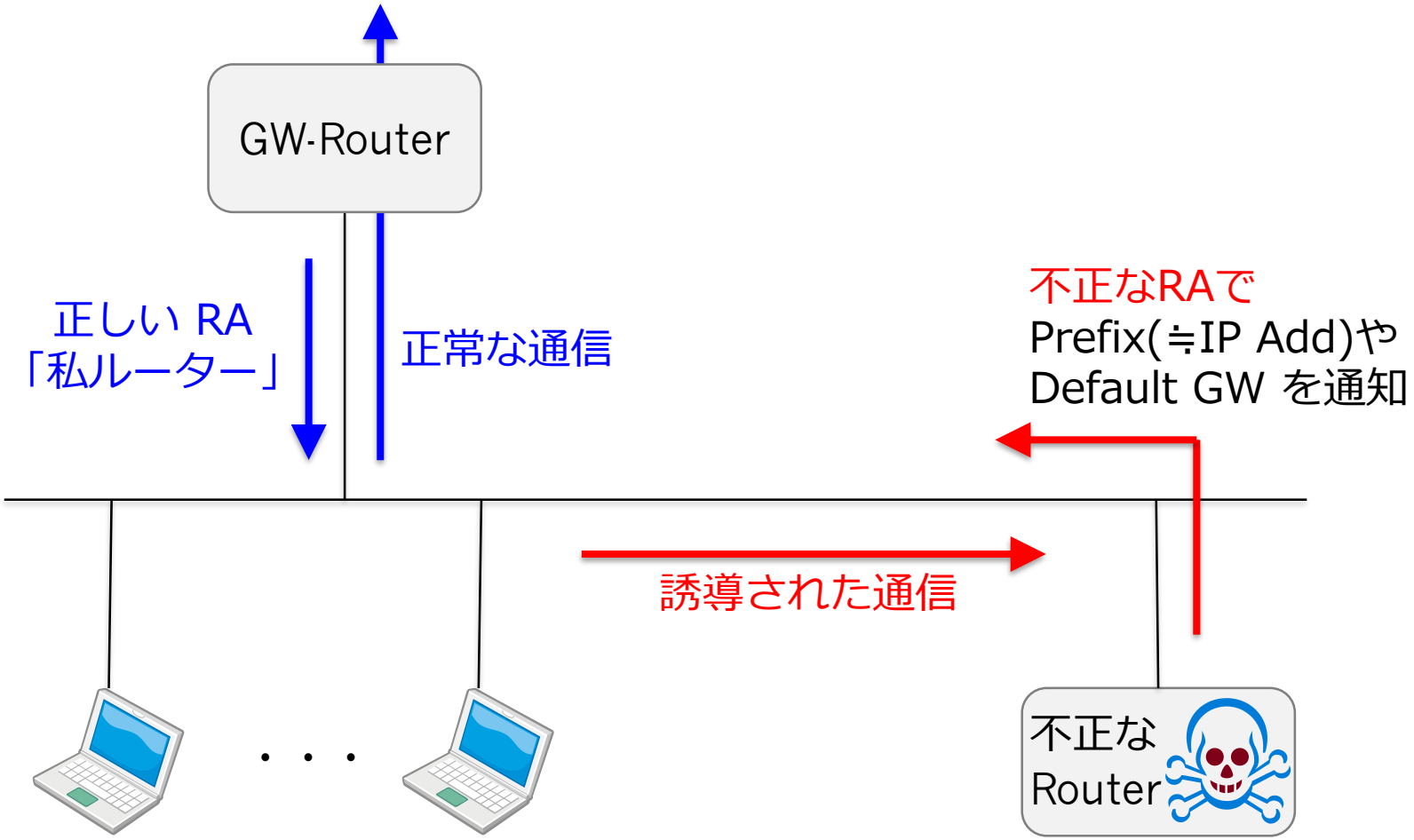
NDP
Neighbor Discovery Protocol

DHCPv6

注
(*1) Link Local Address
(*2) Global Unicast Address

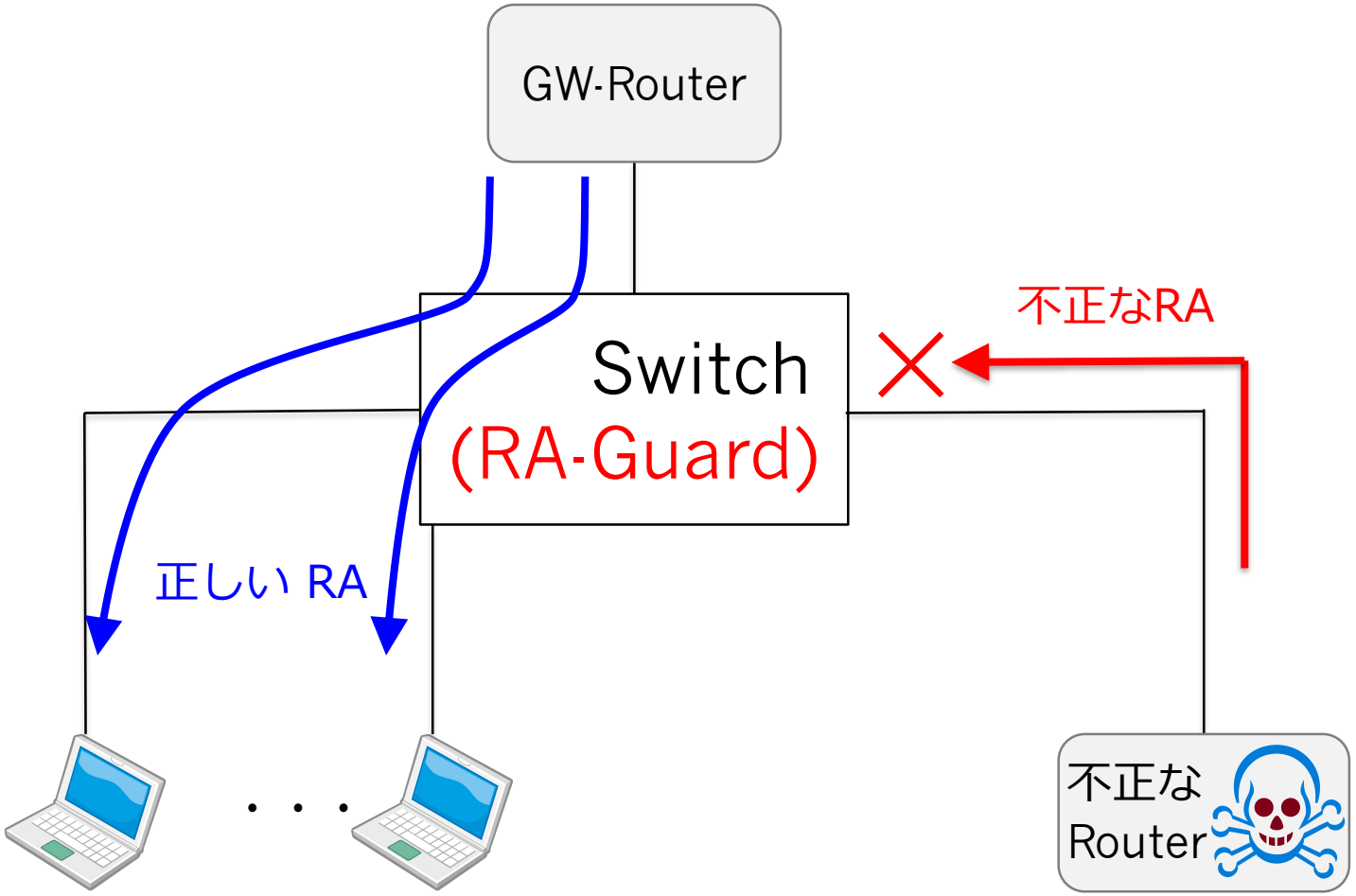
不正RA（Router Advertisement)

- 不正なRAにより、正常な通信ができなくなる。
- NW管理者が NWを IPv4-only にしても、PC等はIPv6が初期設定ONのためにLAN内ではIPv6が動く！



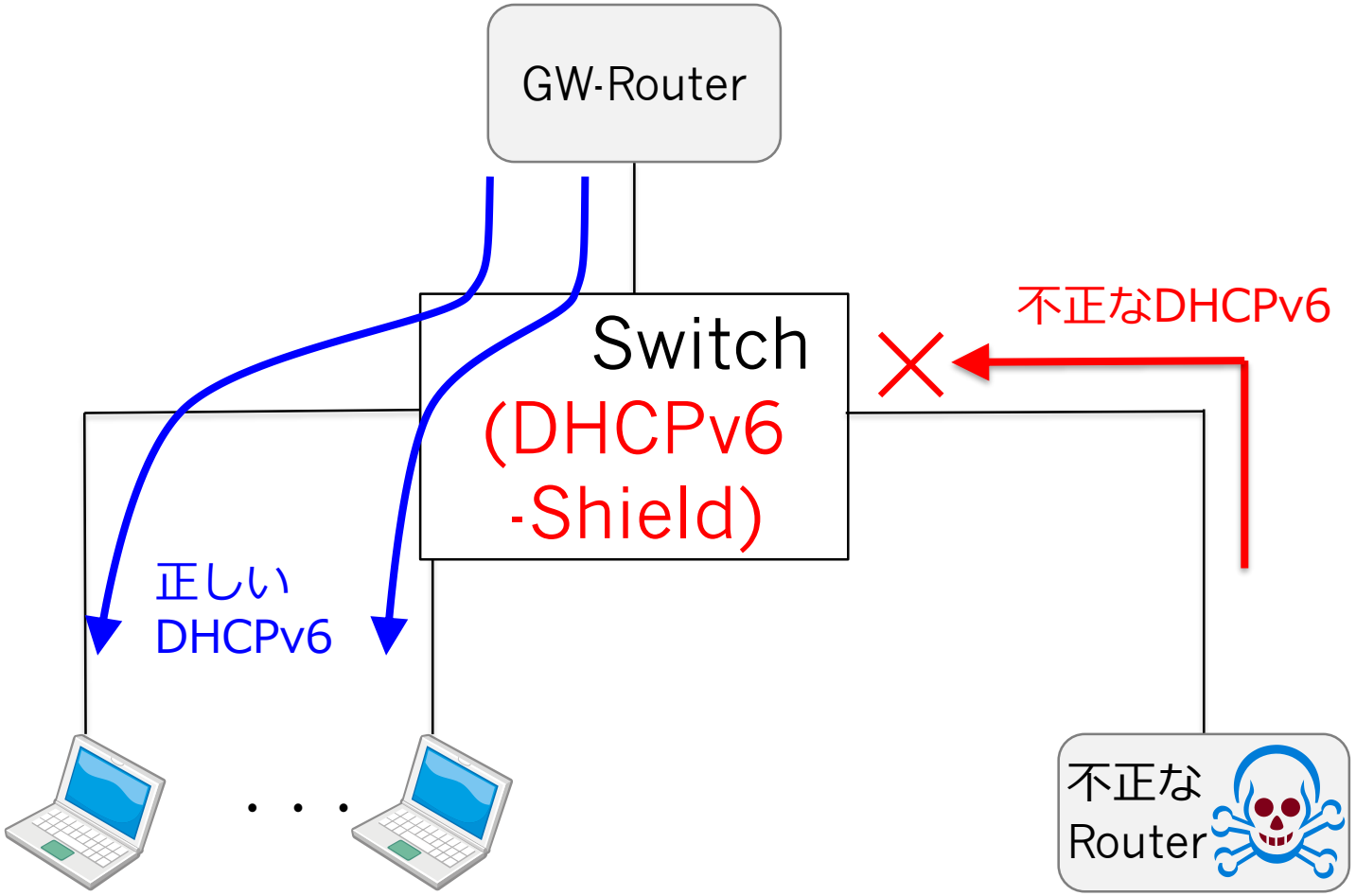
不正RAの対策例

- RA-Guard (RFC6105)を実装しているルーターであれば不正なRAをブロック!
- RA-Guard の実装手法が整理されている。(RFC7113)



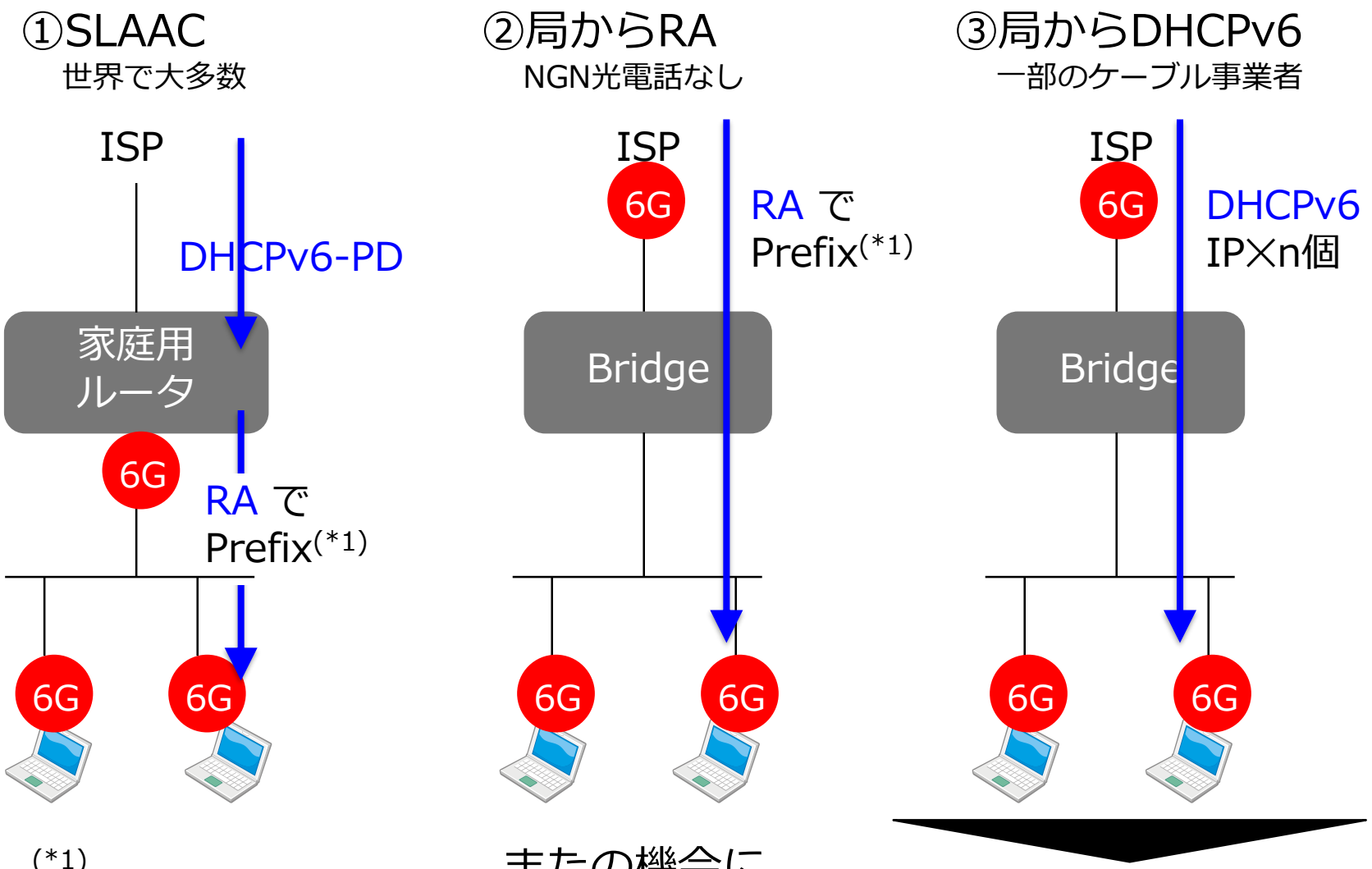
同様に 不正DHCPv6 の対策例

- DHCPv6 においても同様の不正が考えられる。
- DHCPv6-Shield (RFC7610)を実装しているルーターであれば不正なDHCPv6をブロック!



SLAAC以外のIPv6アドレス自動設定

国内では、少なくとも3つの方式が使われている。



DHCPv6の課題

複雑な自動アドレス設定による運用面の課題

東京工業大学 Tokyo Institute of Technology

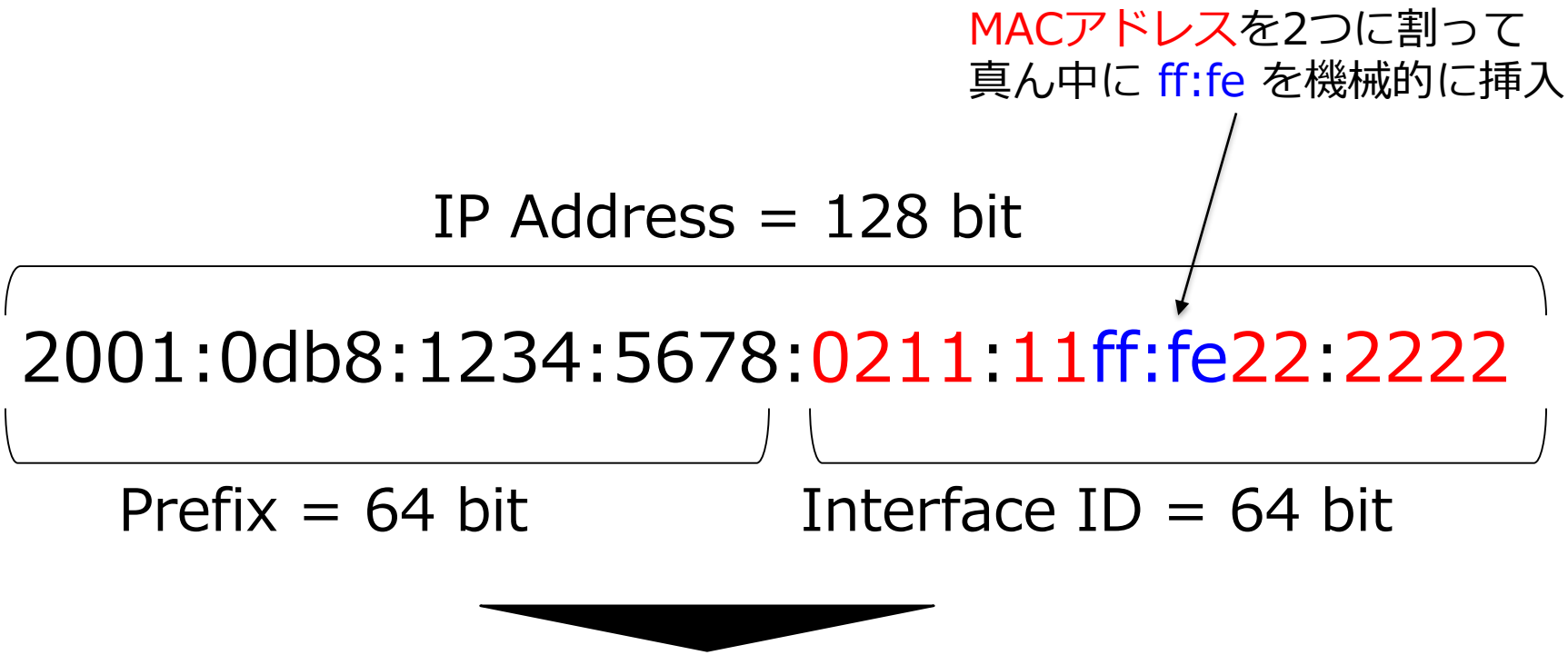
- AndroidにおけるDHCPv6非実装の問題
  - IPv6におけるステートフルアドレス設定が統一的にできない
- Googleの主張（**RFC 7934**）
  - DHCPv6利用はインタフェースに1つのIPv6アドレスと限定することに
    - 1インタフェースに複数のアドレスを持つIPv6の拡張性を害する
    - 1つにするとNAPT利用を助長する

    以上の理由からAndroidでDHCPv6を実装しない
  - 複数アドレスのメリット
    - プライバシ拡張アドレスでトレース回避
    - アプリケーション毎にアドレスを使い分けることが可能
    - テザリングや仮想マシンに対して独立したアドレスを提供可能
- 端末毎の/64利用に関する議論
  - 端末に/64を割り当てる手法（**I-D ietf-v6ops-unique-ipv6-prefix-per-host**）

RFC8273へ !!
2017.12

(プライバシーの問題)
典型的なIPv6アドレス生成 (EUI-64方式)

各端末は、ISPから払い出された Prefix と自インタフェースのMACアドレスを組み合わせて、自らIPアドレスを**自動生成**する。

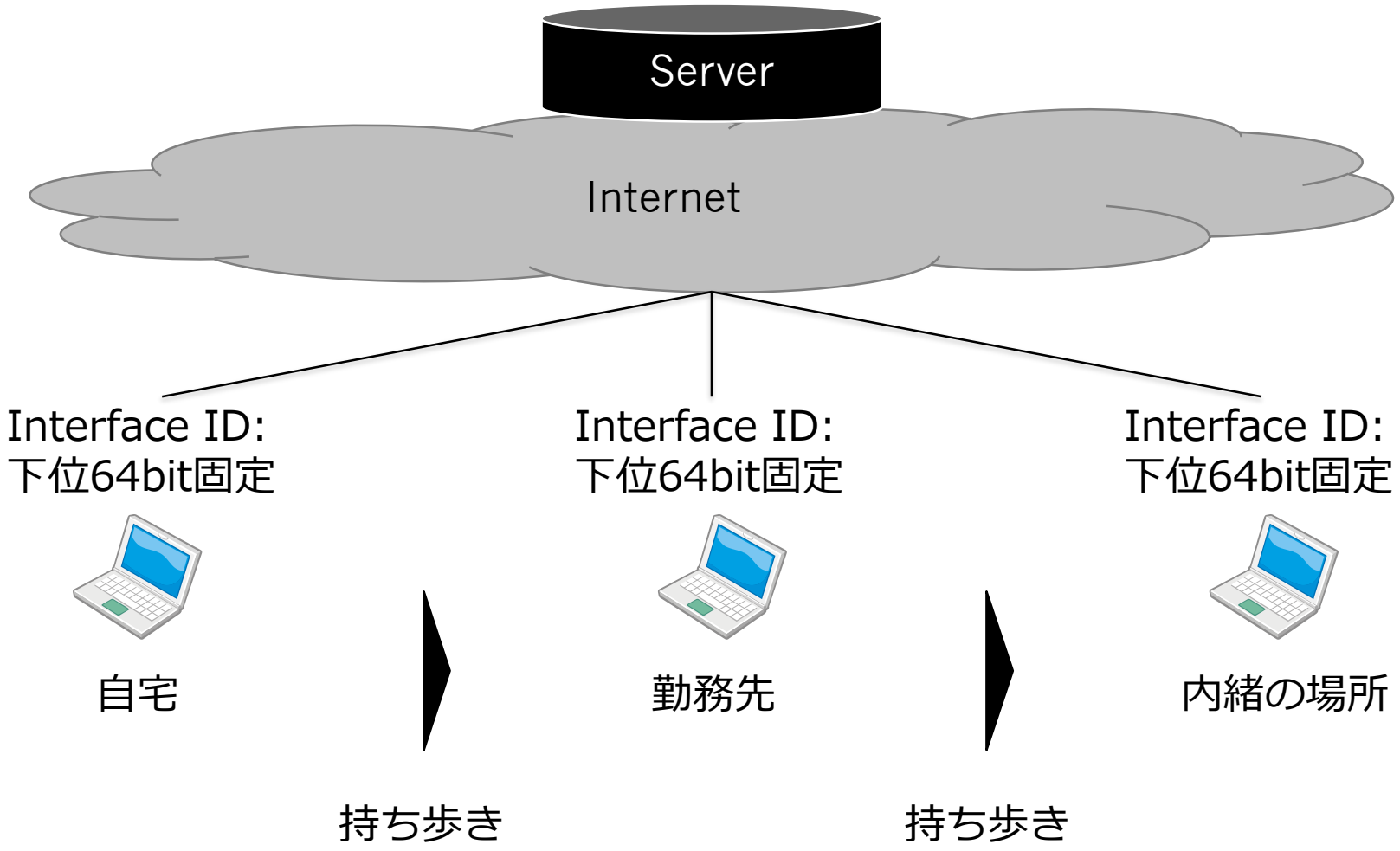


IPv6アドレスの下位64bitが分かれば、
端末(≒端末保有者)を特定できる。

(プライバシーの問題)

EUI-64の問題点

端末保有者はサーバ事業者に訪問先を特定されてしまう。



(プライバシーの問題)

Privacy Extensions for SLAAC

サーバ事業者に端末保有者の訪問先を特定されないために・・・

Privacy Extensions

あるタイミングで下位64bitが変わる。
複数RFC化されている。
(RFC4941・7217・・・)

サーバ管理者は端末の特定が不可

※ 自宅や会社等を特定するためのPrefix(上位64bit)は変わらないため、法執行機関には影響が及ばない。

IPv6アドレスの運用管理とプライバシの問題

IPv6アドレスの運用管理とプライバシの問題

東京工業大学 Tokyo Institute of Technology

- IPv6アドレスフォーマット

- IPv6自動アドレス設定時のIID生成方法の変遷
  - 最初の仕様はMACアドレスからの生成：Modified EUI-64（**RFC 4861**）
    - プレフィックスが変化しても一意に特定可能（プライバシ問題）
    - MACアドレスによる特定機器を狙った攻撃（セキュリティ問題）
  - プライバシ拡張アドレスによるランダム生成の登場（**RFC 4941**）
    - 定期的に変化するためトレーサビリティ確保が困難（管理者視点）
    - 攻撃者にアドレスの匿名性を利用されてしまう問題
  - プライバシを確保しつつ管理性の確保：Semantically Opaque（**RFC 7217**）
    - プレフィックスをIID生成キーの一つとして定義
    - プレフィックス変化でIIDが変わるが同じ環境下では変化しない
      - macOSやLinuxにて実装を確認

※ **RFC 8064**：IID生成手法の仕様を網羅的に解説

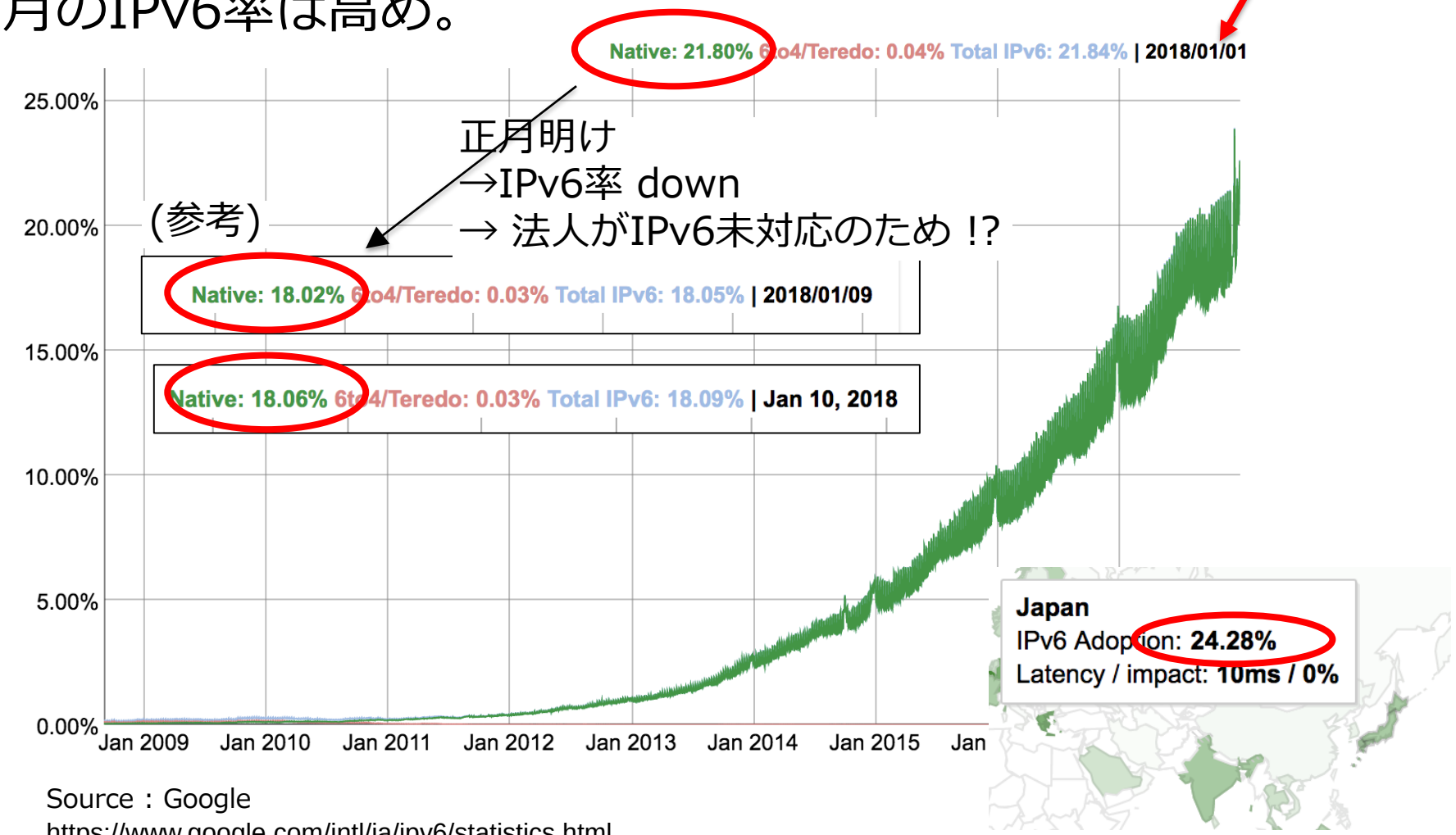
https://www.nic.ad.jp/ja/materials/iw/2017/proceedings/s03/s3-kitaguchi.pdf

目次

- IPv6普及状況
- IPv6のセキュリティー
- **法人のIPv6**

Google への IPv6アクセス率

Google への 全世界からの IPv6アクセス率は 22%
日本からのIPv6アクセス率は 24%
正月のIPv6率は高め。



Source：Google
https://www.google.com/intl/ja/ipv6/statistics.html
https://www.google.com/intl/ja/ipv6/statistics.html#tab=per-country-ipv6-adoption

RFC7381について

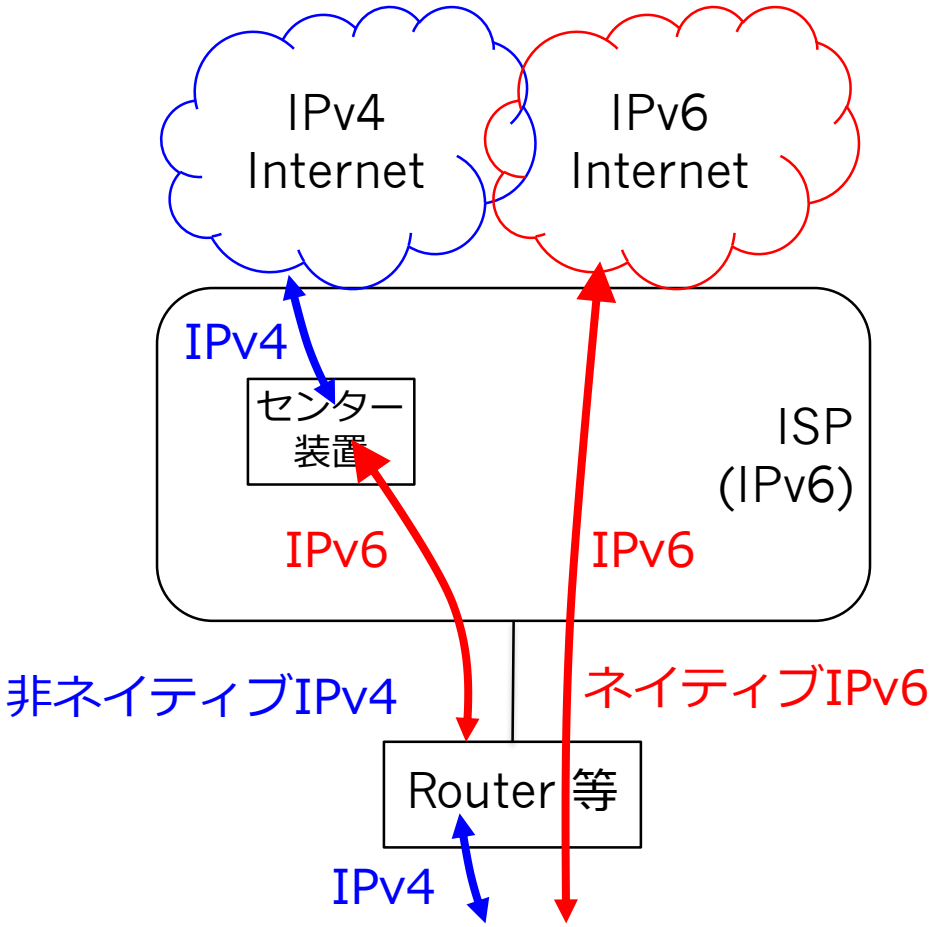
IW2017においては、企業NWについて語られている
RFC7381 に関する紹介がありました。

IPv6導入の最も大きなドライバー

- プロバイダー(固定通信・移動通信)のIPv4枯渇
- ネイティブIPv6及び非ネイティブIPv4 の開始

非ネイティブIPv4通信は以下が考えられる

- NAT64
- NAT444
- DS-Lite (Dual-Stack Lite)
- MAP-T (Mapping of Address and Port using Translation)
- MAP-E (Mapping of Address and Port using Encapsulation)
- その他



(RFC7381の紹介)

IPv4が好ましくない要因

- 性能面
  - パフォーマンスが悪い。
  - 信頼性で劣る。
- 運用面
  - 管理が複雑
  - トラブルシューティングが複雑

補足

- Happy Eyeballs 2 による IPv4 へのペナルティー
- 国内の場合、フレッツはPPPoEの輻輳で、結果的にIPv4が遅い
- アドレス共有していると通らないアプリが有る。(法人の例：一部のTV会議システムが使えない)

- 途中で様々な技術が割り込まれることが多い。
  - トンネル
  - アドレス共有
  - アドレス変換

(RFC7381の紹介)

IPv6導入にかかわらず、IPv4での留意点 - 1/2

公開サーバーでIPv4アクセスのログ取得が必要。(RFC6302 Logging Recommendations for Internet-Facing Serversより)

- ログ取得の理由
  - 犯罪捜査等のためにアドレス共有装置の裏にいる人を特定するため。
  - アドレス共有装置とは、NAT444、MAP、DS-Lite 等を指す。

- 取得項目
  - ソースポート番号
  - タイムスタンプ
  - プロトコル

- ログ取得の際に守るべきこと
  - これらのログは確実に守られていること。
  - プライバシーが守られていること。
  - 定期的にログ保持に関する規則に基づき削除されること。

IPv6導入にかかわらず、IPv4での留意点 - 2/2

IPv6による影響も考慮するべき

- IPv4-only ネットワークにおいてIPv6が動いている場合は注意。最近の端末は初期設定でIPv6対応している。
- 例えば、不正 RA の問題 (前述)は IPv4-only ネットワークで問題を起こす。(RFC6104参照)
- IPv4ネットワークにおける IPv6セキュリティーについては、RFC7123 を参照。

IPv6対応の際に段階的アプローチを行うと良い。

1. 準備・アセスメントフェーズ
   - 全ての管理者にとって必須。後々の失敗や複雑化を防ぐために必要。

2. 外部接続フェーズ
   - enabling IPv6 for Internet-facing systems, as recommended in [RFC5211] 参照

3. 内部接続フェーズ

※ 管理者は 2 と3 のどちらから取り組むかを決めなければならない。

外部接続のIPv6対応・内部接続のIPv6対応の優先順位

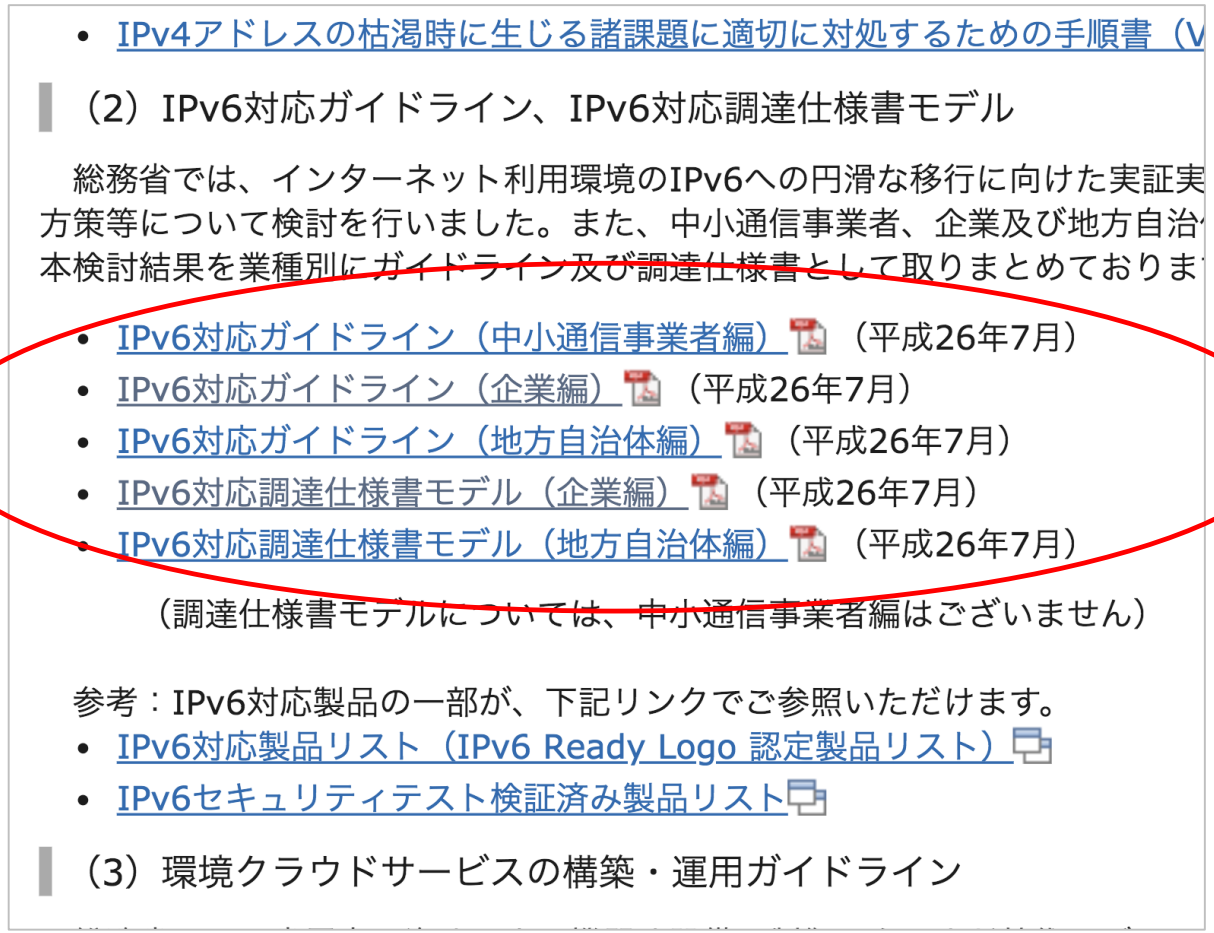
- 多くの場合、外部接続を先に実施。
- たとえ部分的でも外部向けにはIPv6対応しておきたい。

理由

- IPv6の方がTunnelやTranslateを経由してくるIPv4よりパフォーマンスが良い。
- エンタープライズへ通信はシンプルで頑強なIPv6通信が好ましい。

総務省のガイドラインの紹介

総務省のHPで各種のガイドラインが公開されている。



- IPv4アドレスの枯渇時に生じる諸課題に適切に対処するための手順書（V

（2）IPv6対応ガイドライン、IPv6対応調達仕様書モデル

総務省では、インターネット利用環境のIPv6への円滑な移行に向けた実証実
方策等について検討を行いました。また、中小通信事業者、企業及び地方自治
本検討結果を業種別にガイドライン及び調達仕様書として取りまとめておりま

- IPv6対応ガイドライン（中小通信事業者編）（平成26年7月）
- IPv6対応ガイドライン（企業編）（平成26年7月）
- IPv6対応ガイドライン（地方自治体編）（平成26年7月）
- IPv6対応調達仕様書モデル（企業編）（平成26年7月）
- IPv6対応調達仕様書モデル（地方自治体編）（平成26年7月）

（調達仕様書モデルについては、中小通信事業者編はございません）

参考：IPv6対応製品の一部が、下記リンクでご参照いただけます。

- IPv6対応製品リスト（IPv6 Ready Logo 認定製品リスト）
- IPv6セキュリティテスト検証済み製品リスト

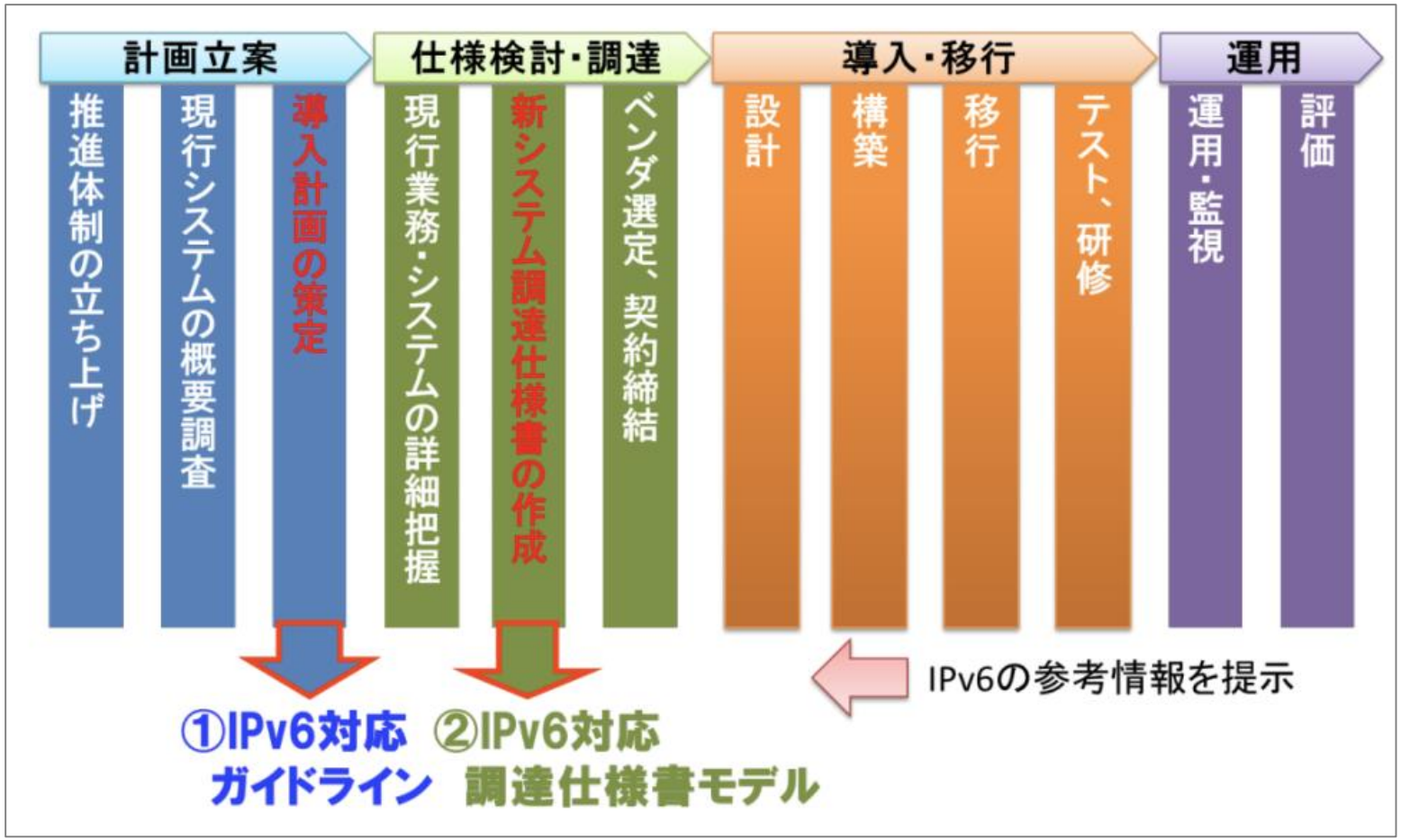
（3）環境クラウドサービスの構築・運用ガイドライン

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

(総務省のドキュメント紹介)

「ガイドライン」と「仕様書調達モデル」の位置付け

両ドキュメントは、IPv6対応計画立案及び製品等の調達の際に有用。



http://www.soumu.go.jp/main_content/000301466.pdf

(総務省のドキュメント紹介)

「ガイドライン」と「仕様書調達モデル」の内容

セットで利用することを想定している。

- ガイドライン
  - IPv6 対応の方法や検討上の留意点等を説明している。
  - 基本計画を作成することができるようになっている。

- 仕様書調達モデル
  - 調達仕様書のモデルを提示している。
  - それぞれの企業 に応じた調達仕様書を作成できると考えている。

(総務省のドキュメント紹介)

IPv6 対応ガイドライン 【企業編】より抜粋

自らが必要な情報を抜粋して得ることが可能。

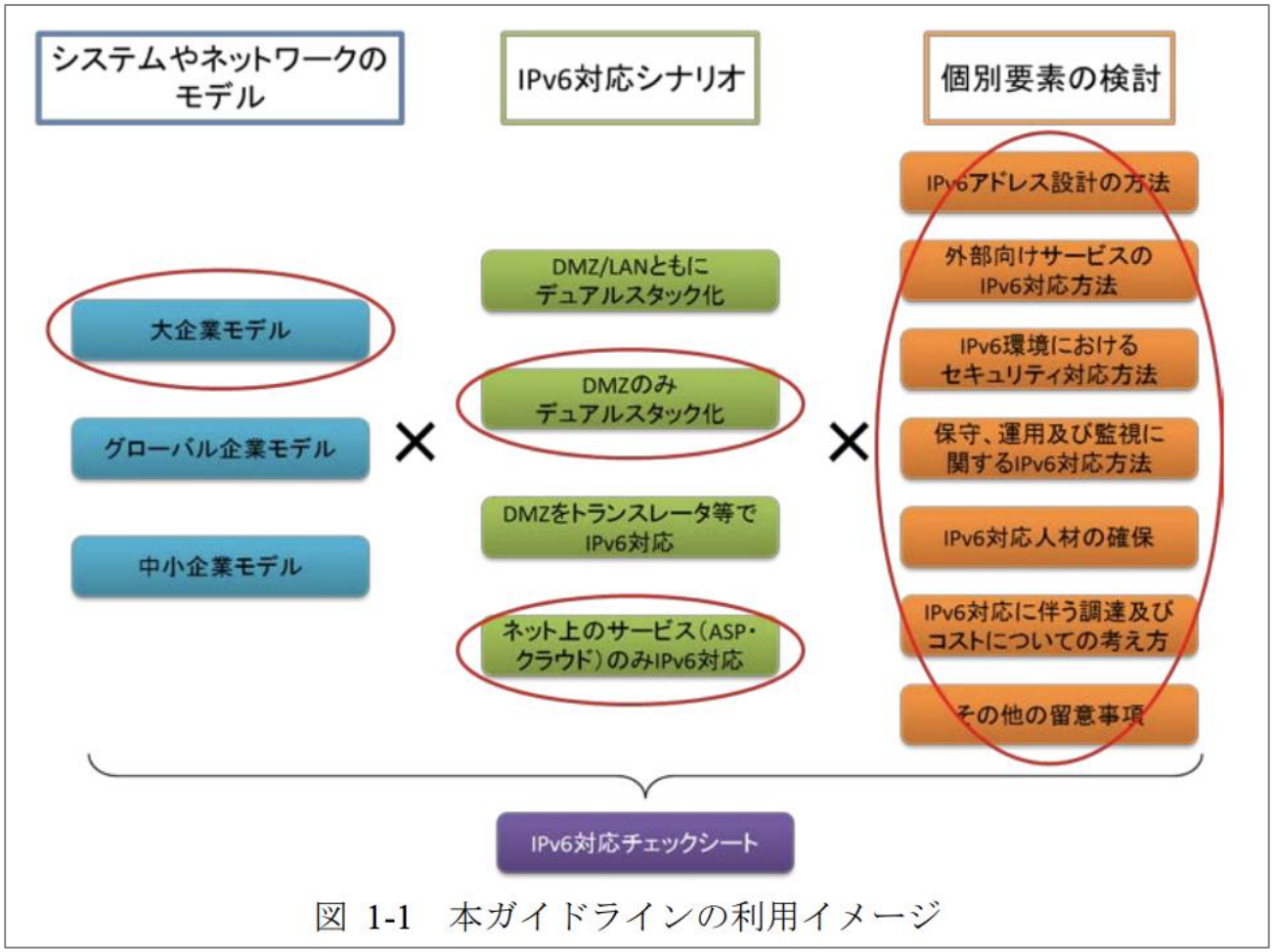


図 1-1 本ガイドラインの利用イメージ

http://www.soumu.go.jp/main_content/000301464.pdf

(総務省のドキュメント紹介)

「ガイドライン」具体的内容 (抜粋)

IPv6 アドレスの調達方法

A) ISPから

- 上位ISPのグローバルアドレスの一部
- 一般的な組織であればこれで十分

B) JPNIC等から

- 組織専用のグローバルアドレス
- 上位ISPに依存せずに自らNWを運用する場合や特殊なNWを運用する場合など。

その他幅広く記載されている。

- 組織内でのアドレスの使い方
- アドレスの管理方法
- DMZにおけるアドレスの使い方の留意点　などなど

http://www.soumu.go.jp/main_content/000301464.pdf

(総務省のドキュメント紹介)

IPv6 対応調達仕様書モデル 【企業編】より抜粋

機器毎の調達仕様のモデルが記載されている。
(「・・・ができること。」などのリスト)

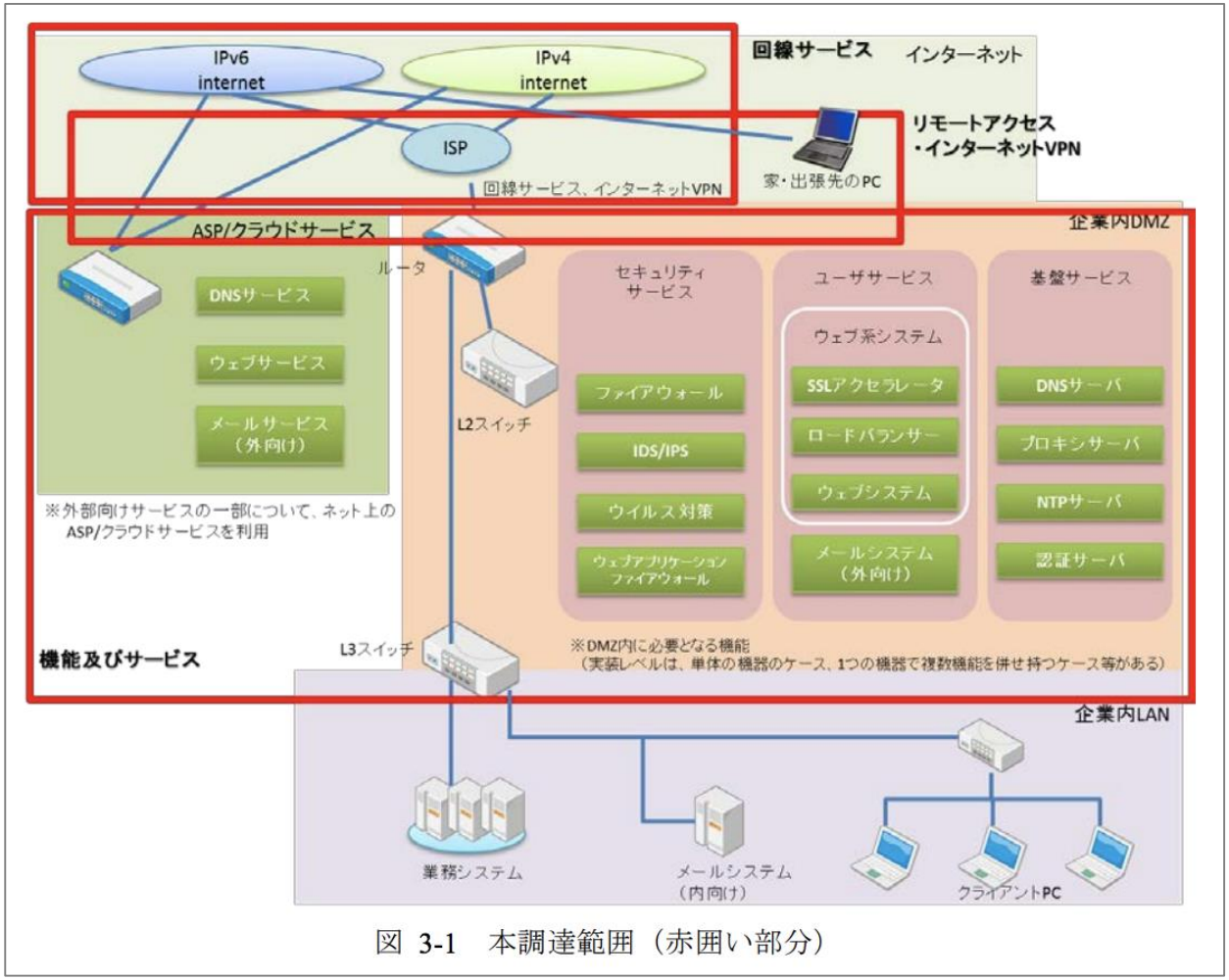


図 3-1 本調達範囲（赤囲い部分）

http://www.soumu.go.jp/main_content/000301466.pdf

(総務省のドキュメント紹介)

「調達仕様モデル」具体的内容 (抜粋)

ロードバランサーの例：

- ロードバランサーとして備えるべき基本機能を有すること。
- IPv4/IPv6 通信が可能であること。
- 外部からの IPv4/IPv6 によるアクセスをウェブサーバに振り分ける際に、ウェブサー バに対する通信を IPv4 及び IPv6 のいずれかを選択できること。
- IPv4 通信と IPv6 通信が同等のスループットを処理できる能力を有すること。
- IPv4 通信と IPv6 通信が同等の TLS/SSL のアクセラレータの性能を有すること。
- 冗長構成を取ることで IPv4/IPv6 通信の冗長化を可能とする機能を有すること。
- IPv4/IPv6 通信による運用管理端末からのリモート保守を可能とする機能を有するこ と。
- IPv4/IPv6 通信による時刻設定を常時正しい状態に保つことを可能とする機能を有す ること。
- IPv4/IPv6 通信の情報をログ出力できること。
- ログ出力の通信に IPv4/IPv6 通信が利用できること。
- 【OP】IPv4/IPv6 通信による構成定義情報のバックアップを可能とする機能を有する こと。
- 運用管理を行うネットワークで IPv6 対応を行う場合。

http://www.soumu.go.jp/main_content/000301466.pdf

最後に

現在のIPv6とIPv4

世界において IPv6対応と IPv4の劣化は同時に起きています。

IPv6導入

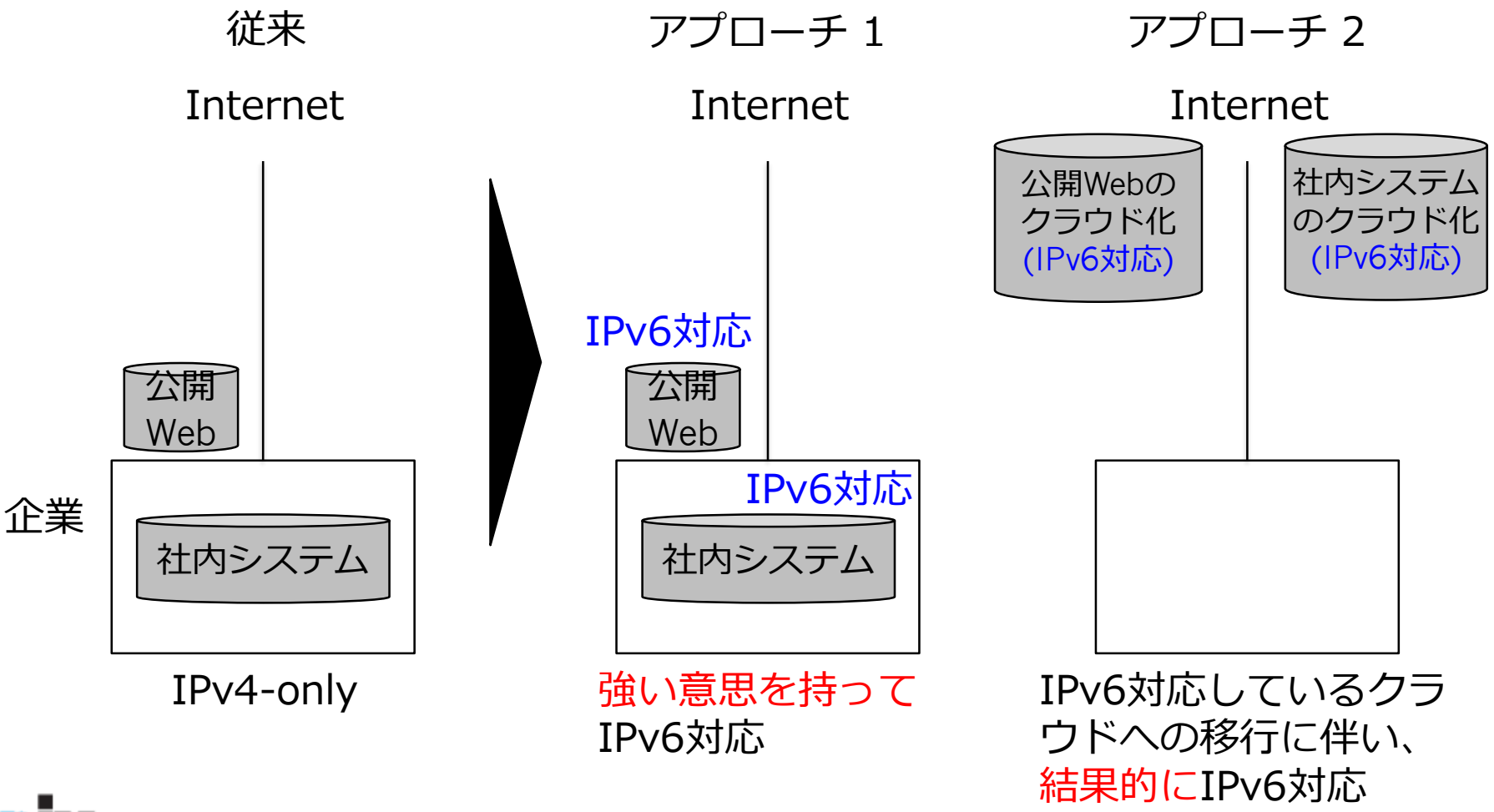
- USを中心とする大手クラウド事業者のIPv6対応急加速
- USを中心とする大手PC・モバイル・OS のIPv6対応急加速
- 上記事業者の世界進出
- 各国NW事業者のIPv6対応

IPv4劣化

- 標準化団体によるIPv4劣化
- IPv4アドレス共有による技術的課題
- 無数に存在するIPv4の共有方式に対応するためのクラウド・端末・アプリのコスト増
- 国内においては、フレッツ IPv4 PPPoE の輻輳

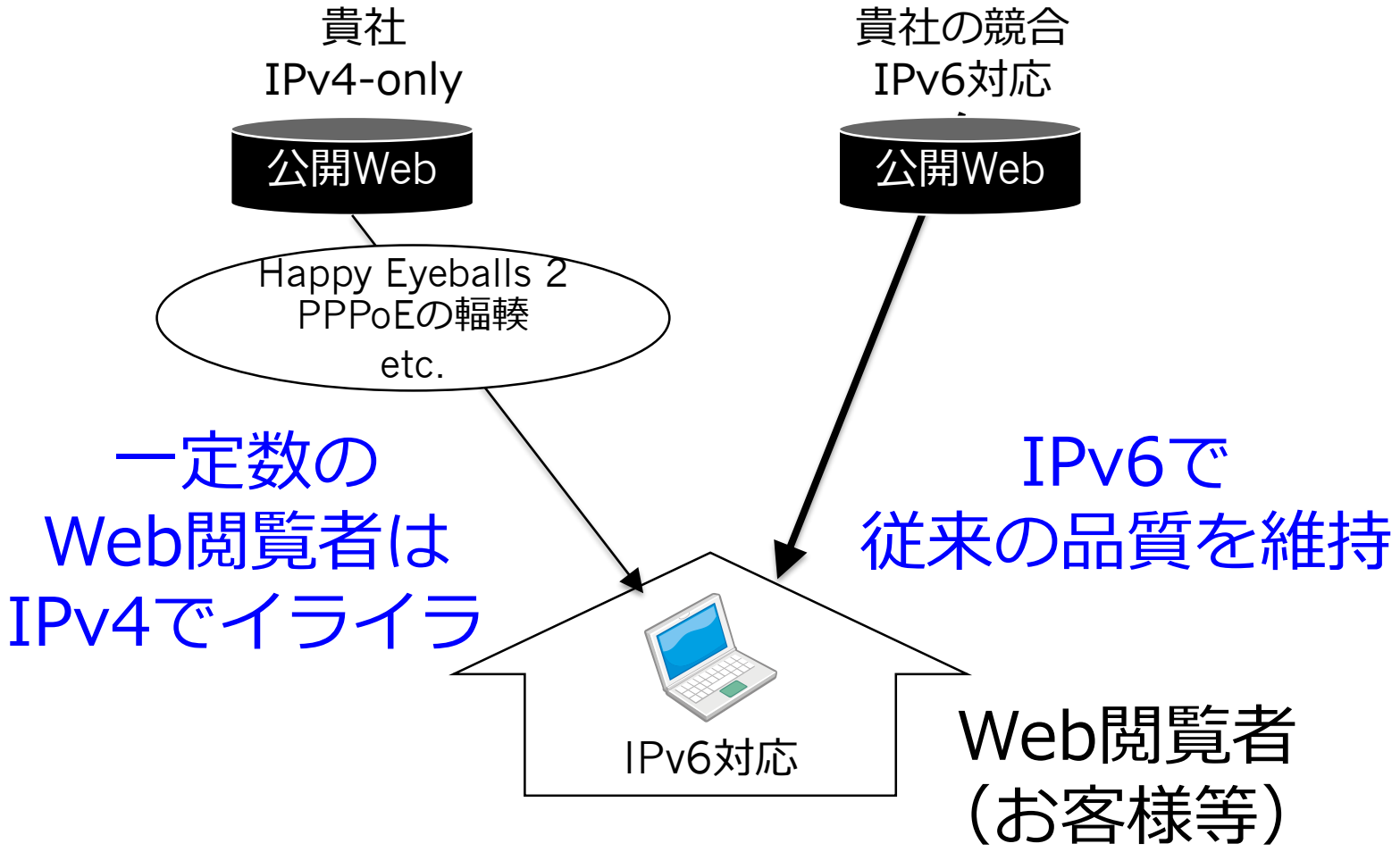
企業ネットワークの2つのIPv6アプローチ

(話者の見解)
多くの場合、2つのアプローチの混在になるであろう。
中小の企業はアプローチ2のみでのIPv6自然対応へ。



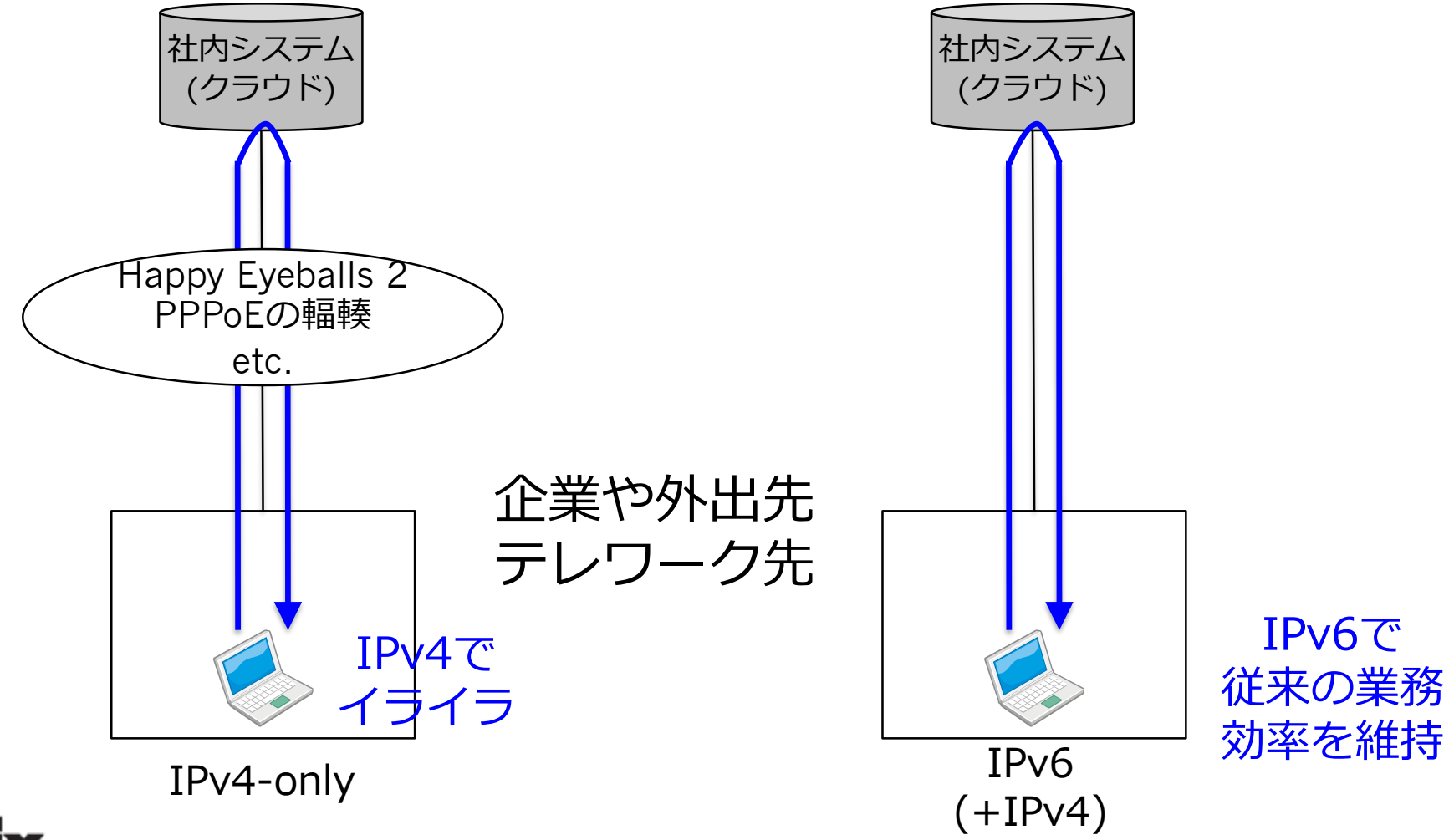
まずは、公開Webだけでも。

まずは、お客様視点で 公開Webから IPv6対応を。
但し、目的をIPv6とすると、社内でのIPv6化は撃沈となります。
クラウド化のタイミングがチャ～ンス !!



本質的には今後の企業NWにはIPv6が適している

社内システムのクラウド化に伴い、従業員のクリックや入力に伴う全ての通信がクラウドを往復する。




jpix