Internet Week 2018
Internet Week流 Security Bootcamp
D1-1 常識変化に向き合おう

知っておくべきIPv6とセキュリティの話

2018.11.27

日本インターネットエクスチェンジ㈱

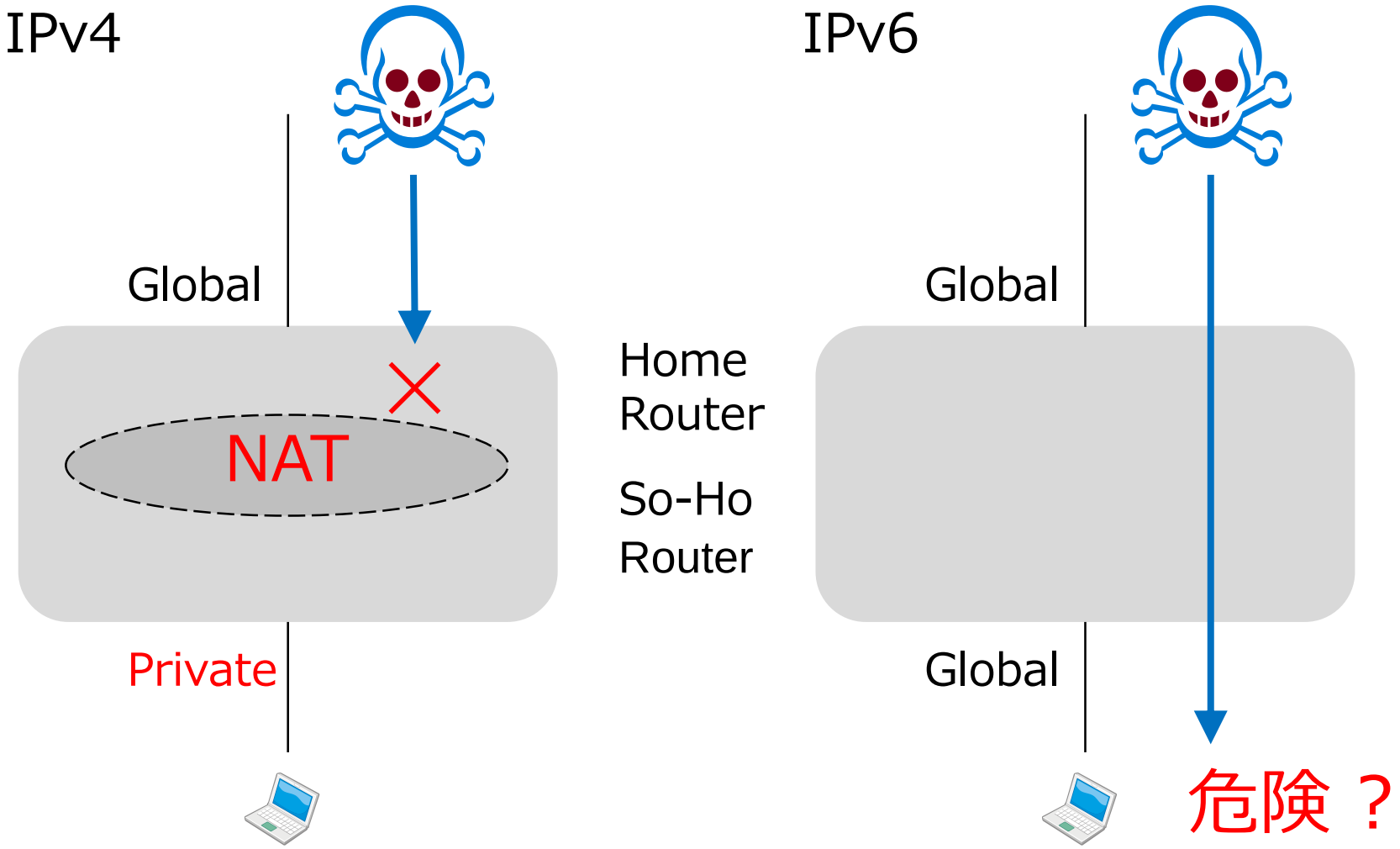
a-nakagawa at jpix dot ad dot jp

中川あきら

目次

(ウォーミングアップ)

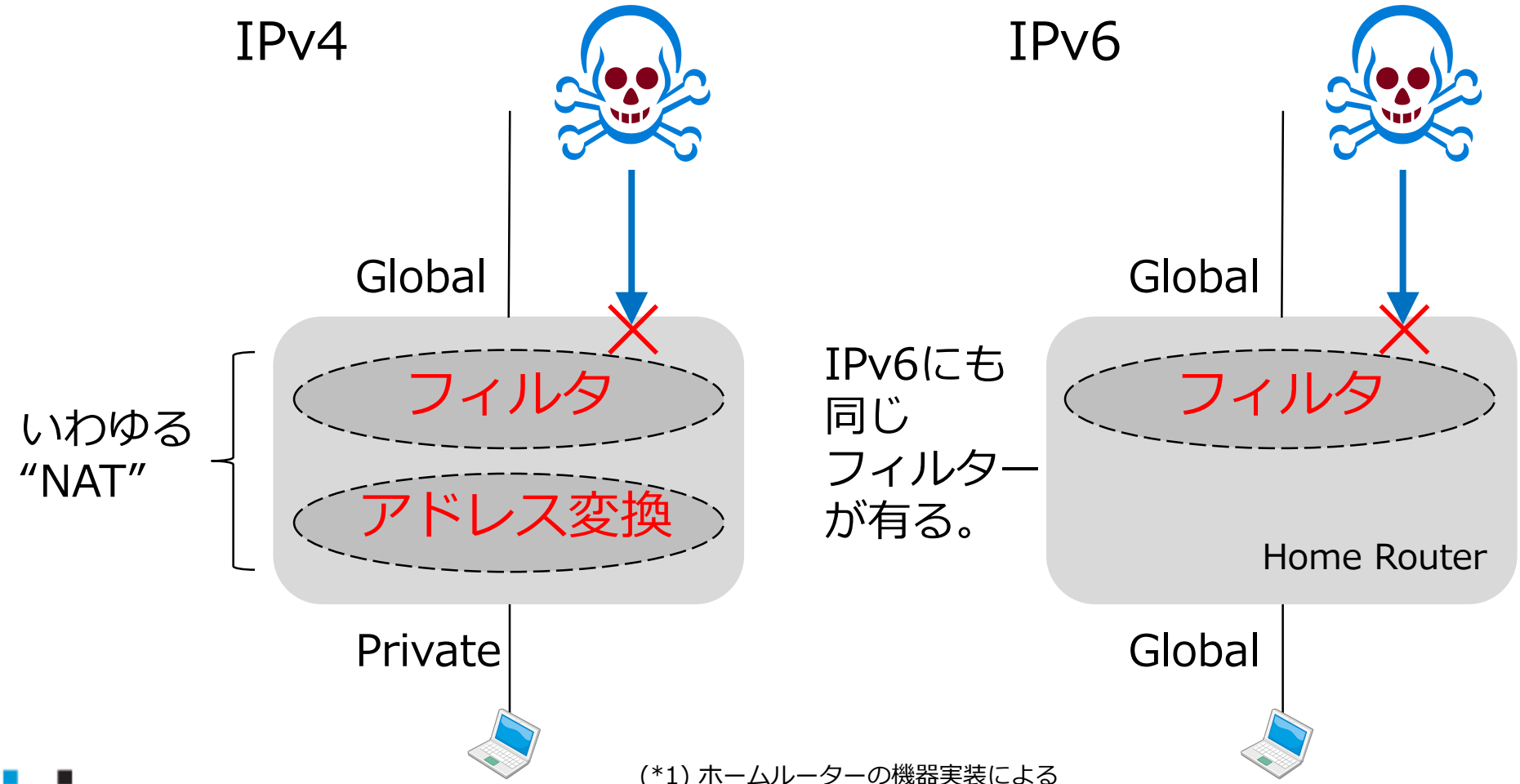
「IPv6はNATが無いから危険」ですか ???



(ウォーミングアップ)

「IPv6はNATが無いから危険」ではありません！

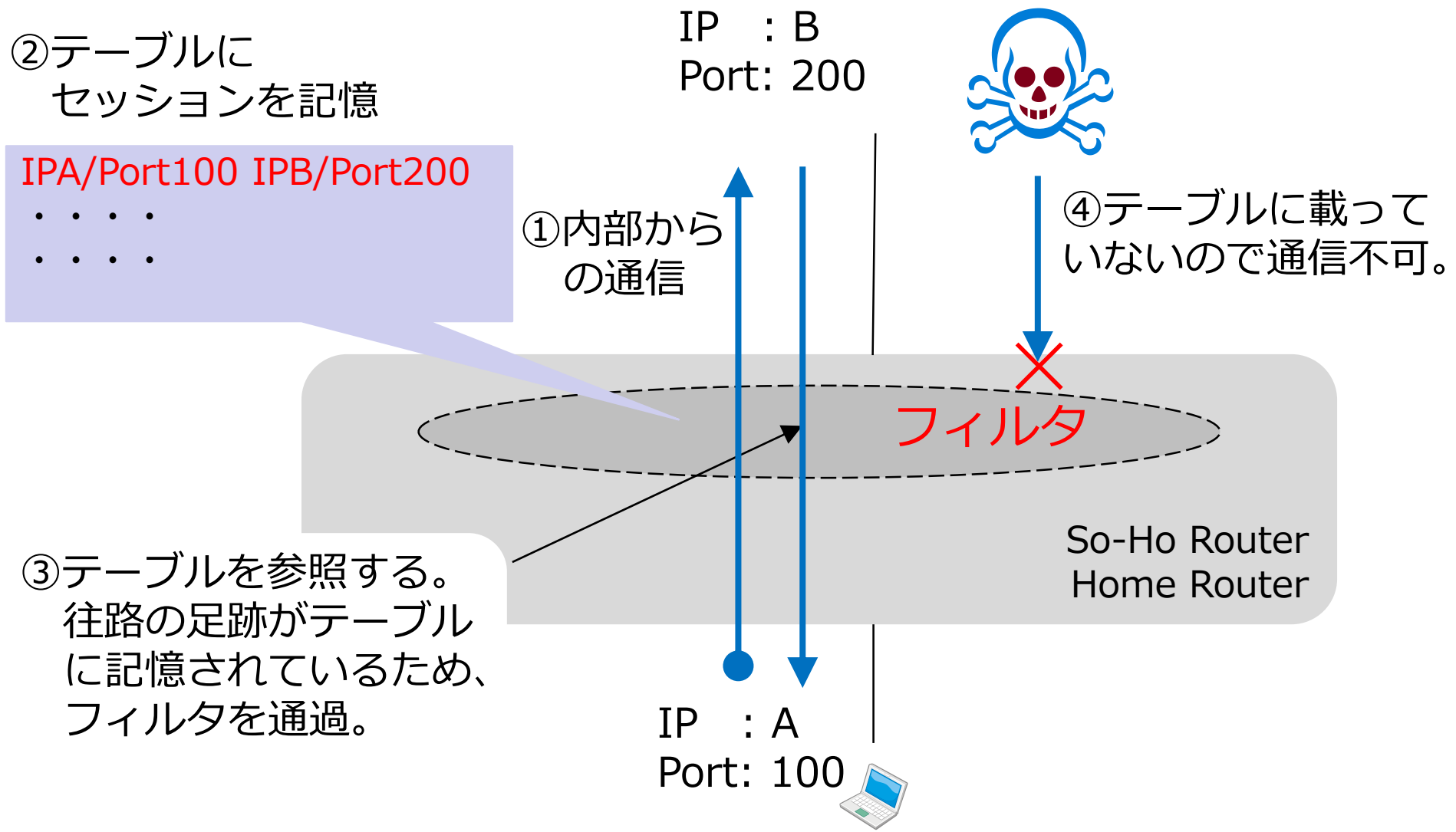
IPv6 には IPv4 と同等のフィルターがあります。(*1)
IPv6 にアドレス変換機能が無いだけです。



(*1) ホームルーターの機器実装による

(ウォーミングアップ)

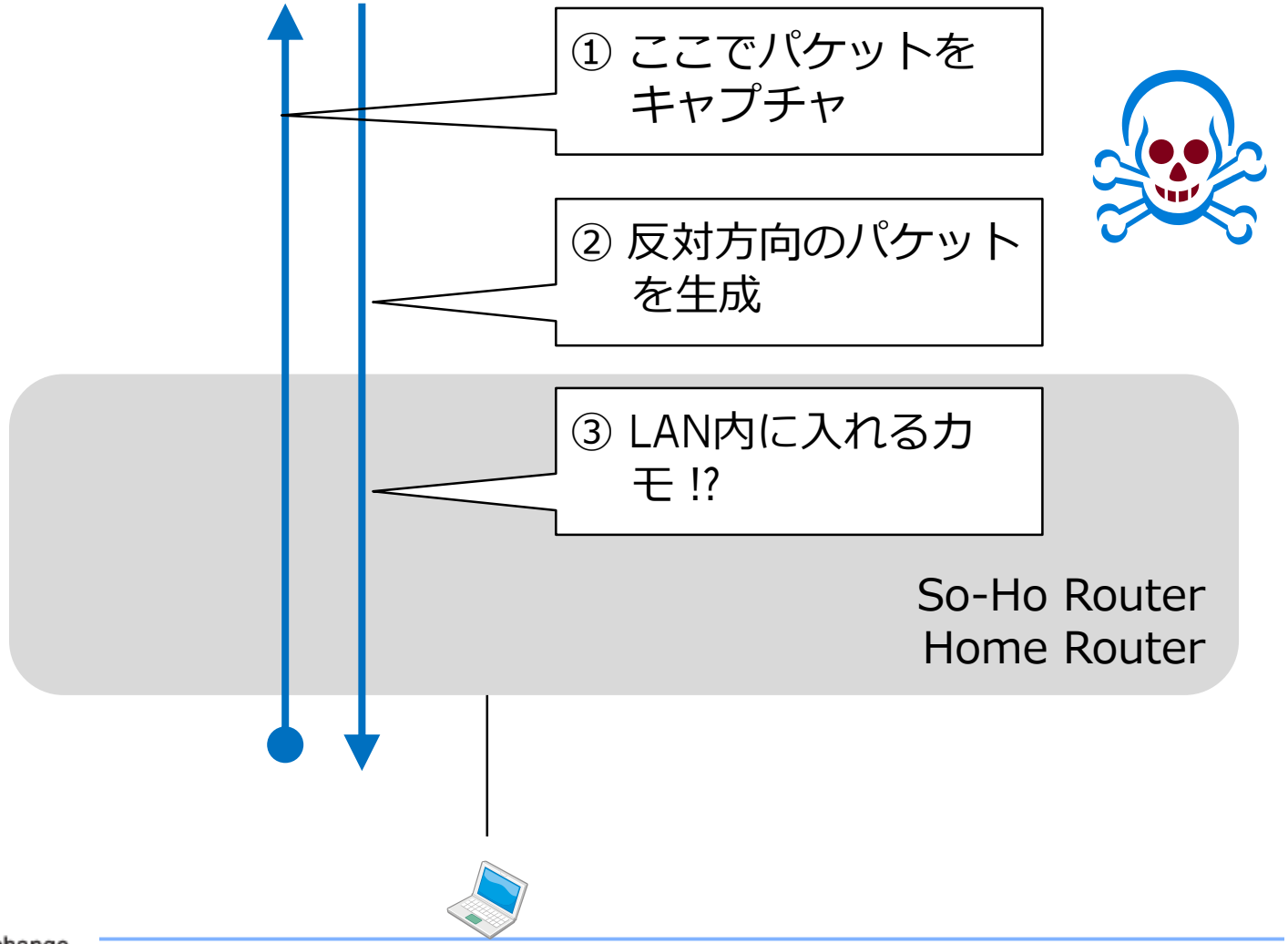
フィルタ機能の考え方(IPv4・IPv6共通)



(ウォーミングアップ)

「IPv6もIPv4もフィルタがあるから安全」ですか ???

IPv6 も IPv4 も同じく安全とは言い切れません。
例えば・・・

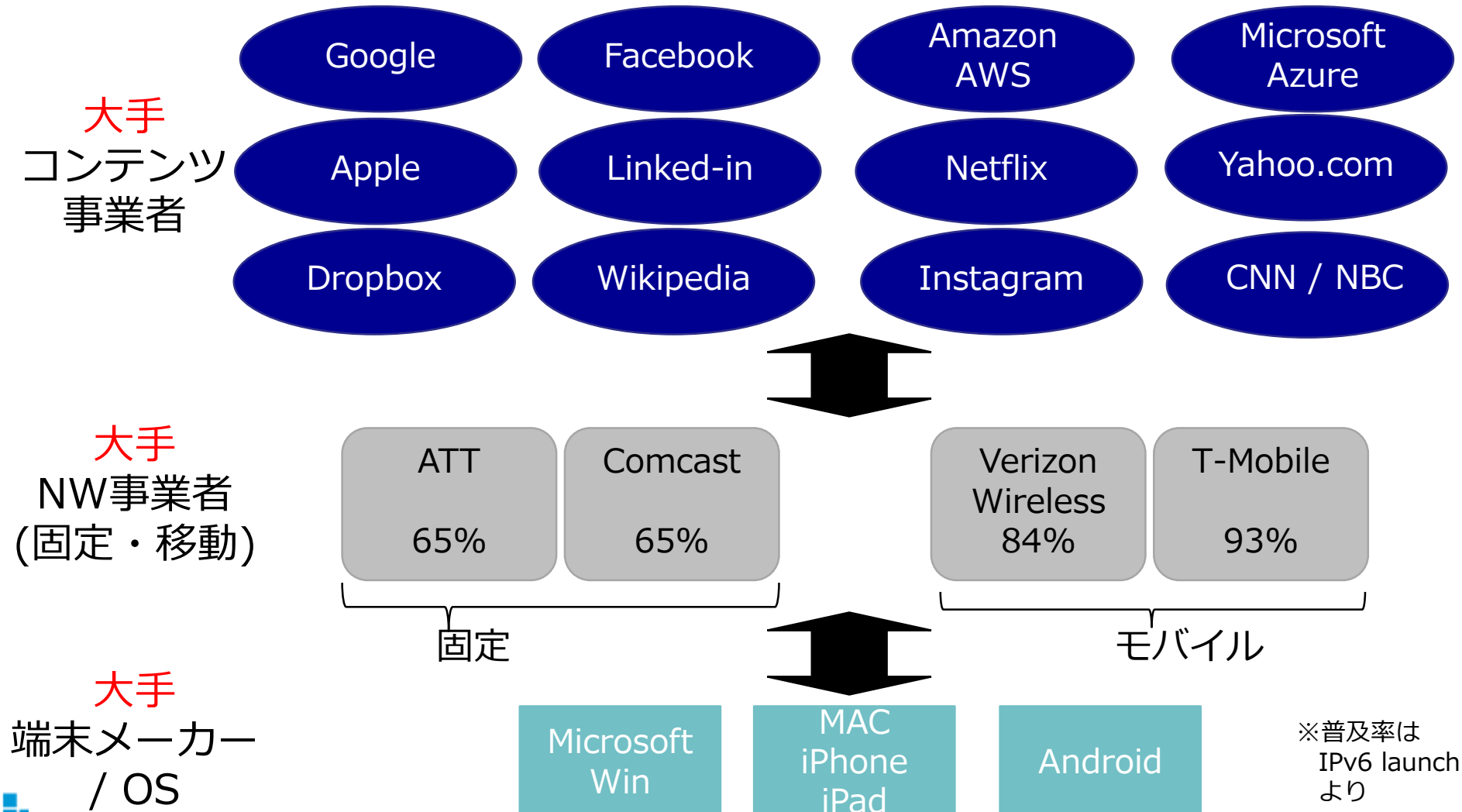


目次

- ウォーミングアップ
- **IPv6セキュリティーのモチベーション**
- LAN編
- Home Router のフィルター編
- プライバシー編
- ICMPv6編
- IPv4アドレス共有の影響編

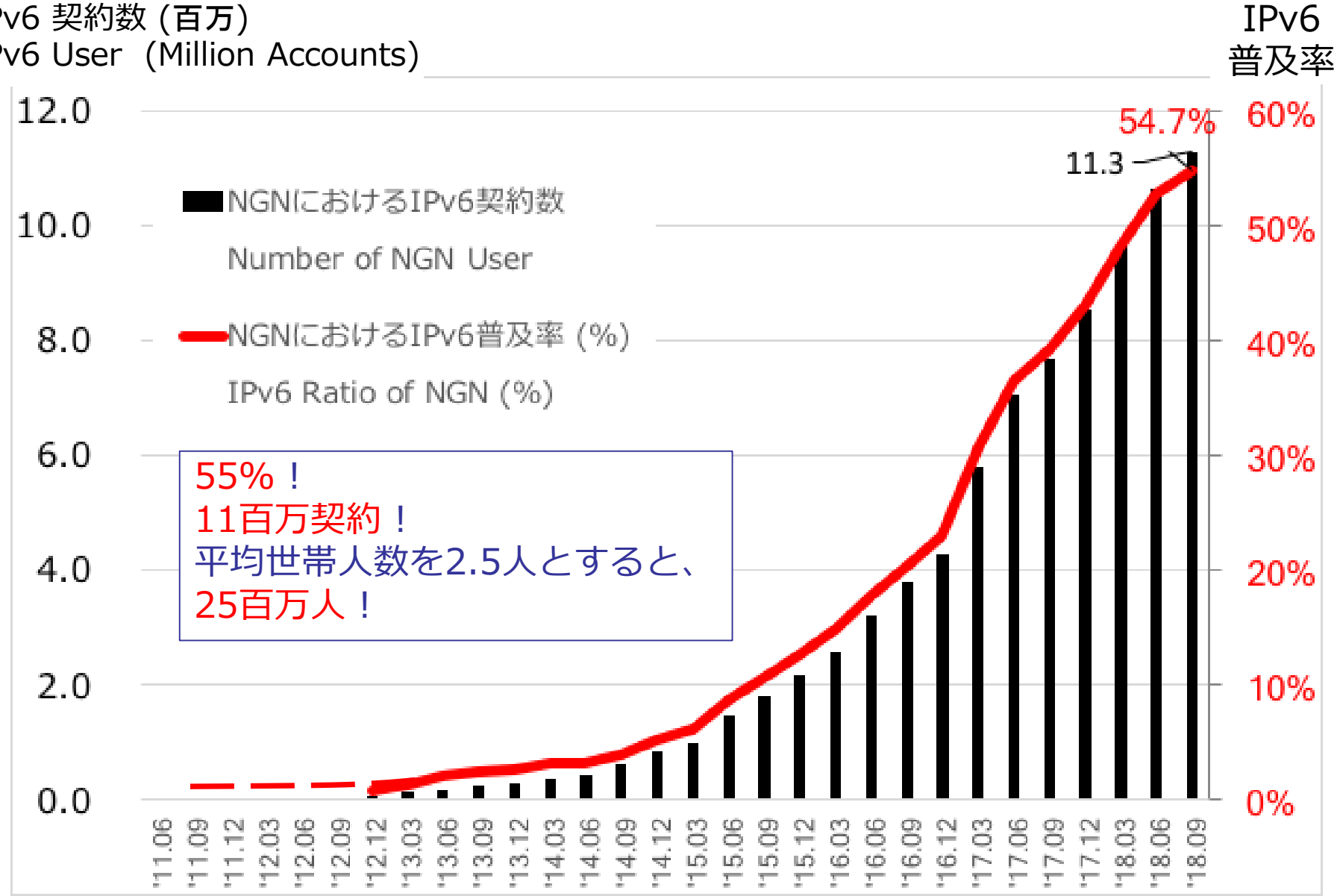
USの主要プレーヤーのIPv6対応状況

各プレーヤーが、すさまじいスピードでIPv6対応中。
→ 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

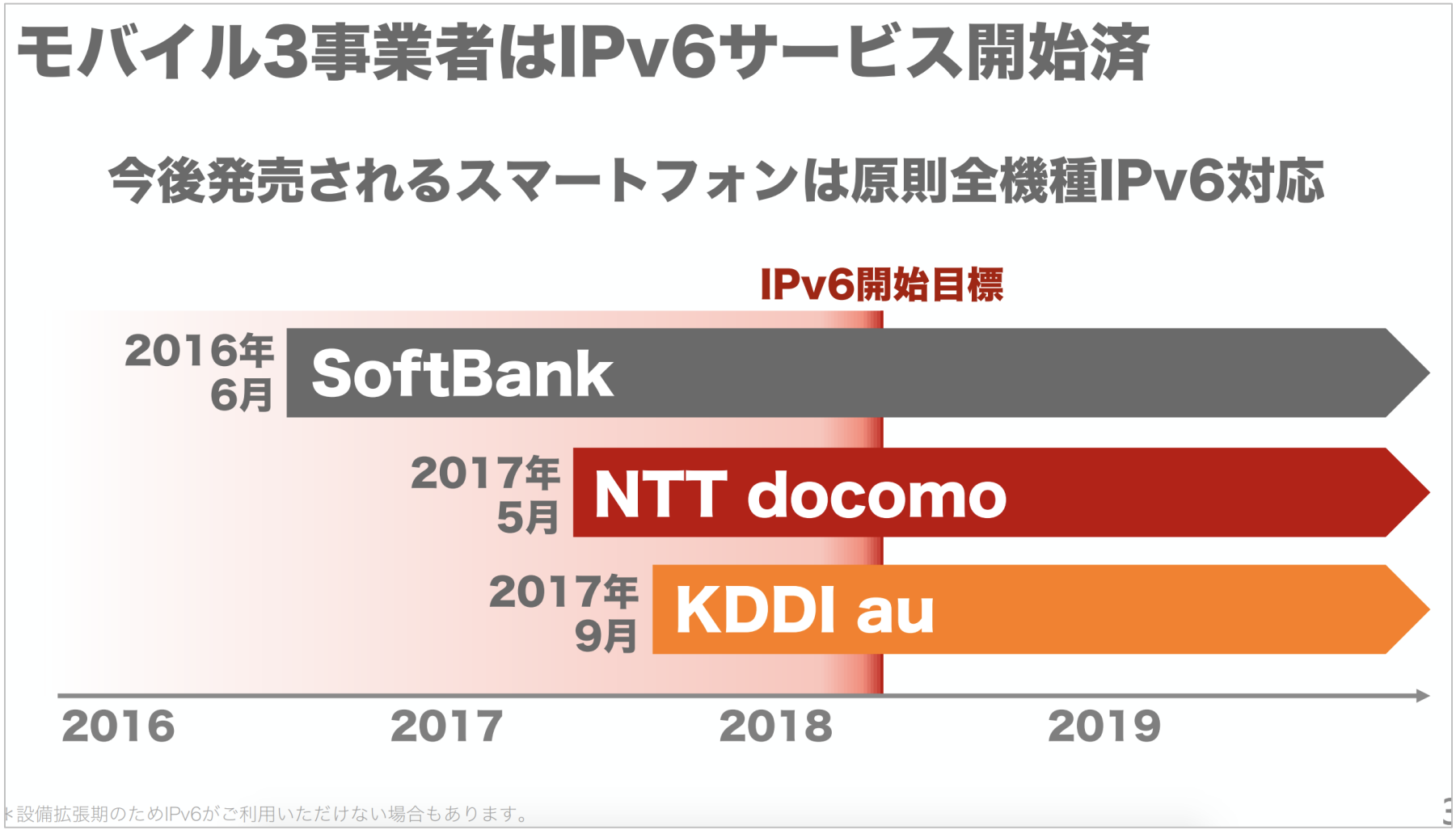
国内で進むIPv6・NGNにおけるIPv6対応状況



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

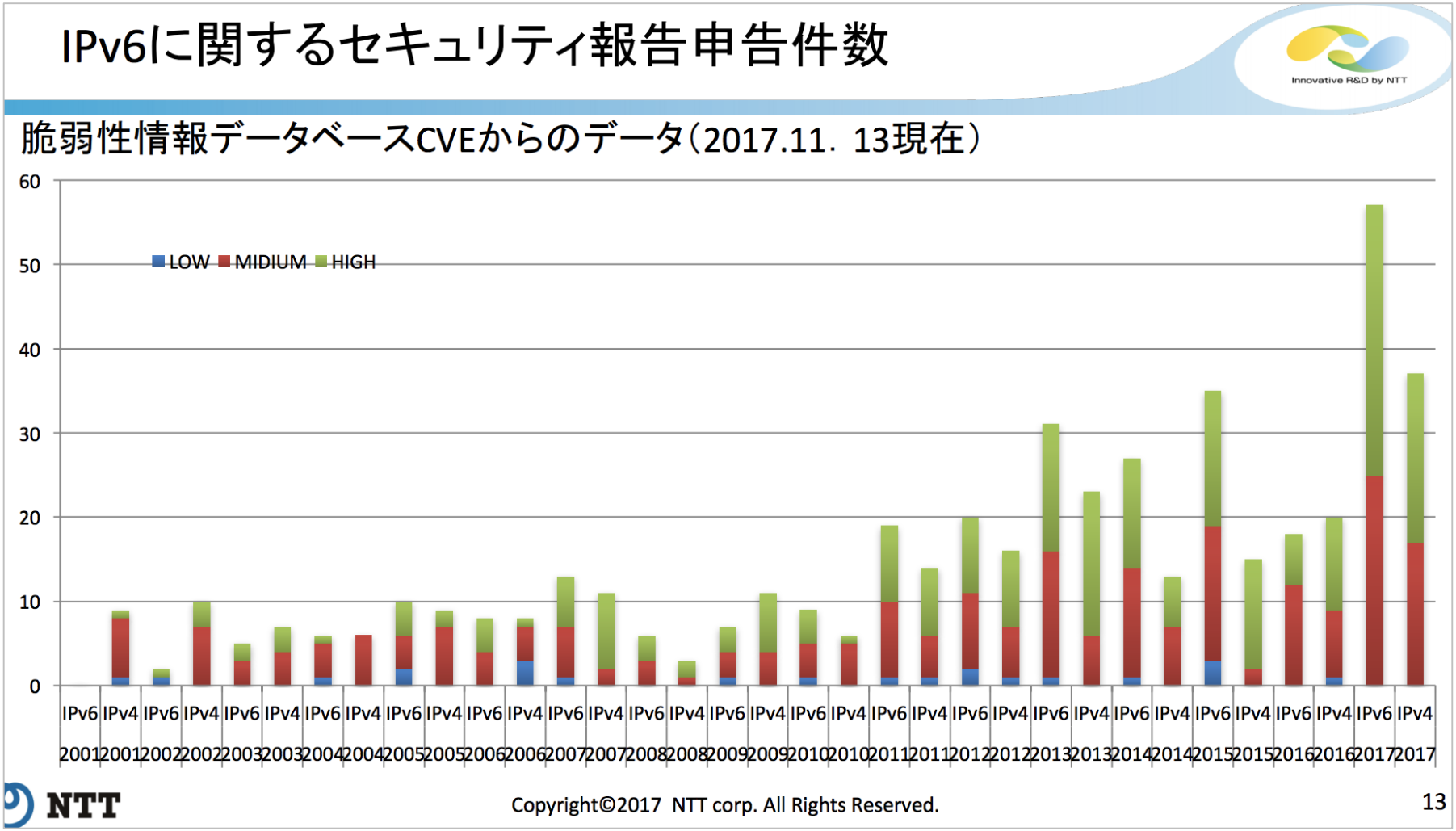
国内で進むIPv6・モバイル3社

本格対応開始 !!



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

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

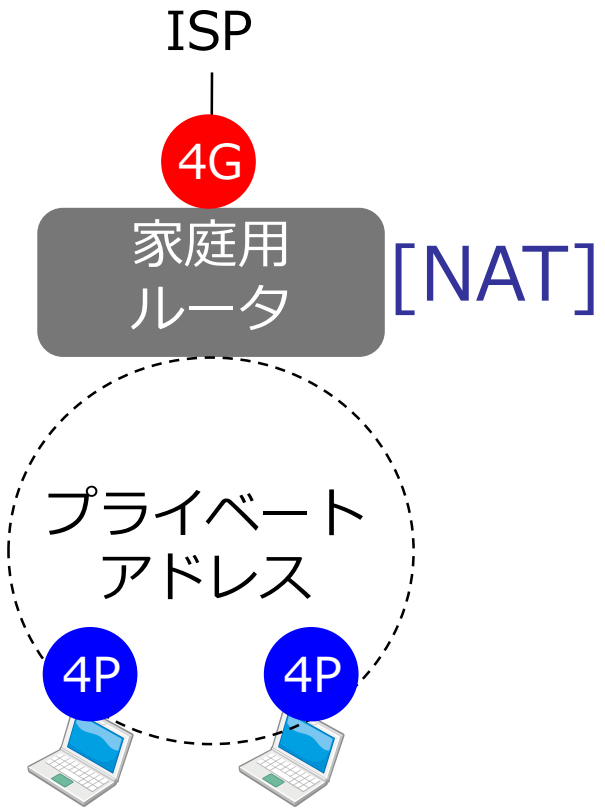
目次

- ウォーミングアップ
- IPv6セキュリティーのモチベーション
- **LAN編**
- Home Router のフィルター編
- プライバシー編
- ICMPv6編
- IPv4アドレス共有の影響編

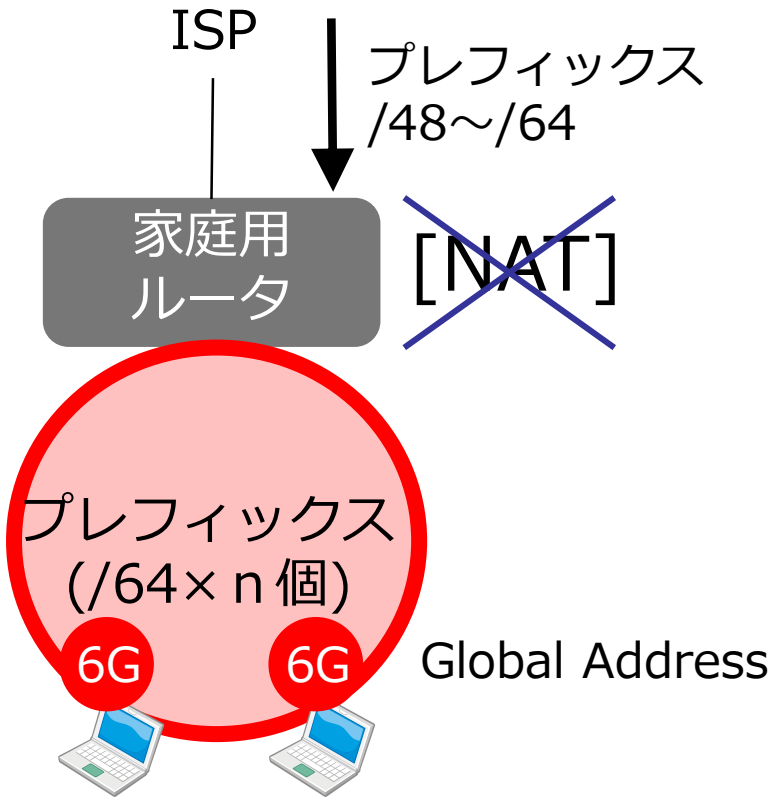
IPv4とIPv6のアドレス払い出しの考え方

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

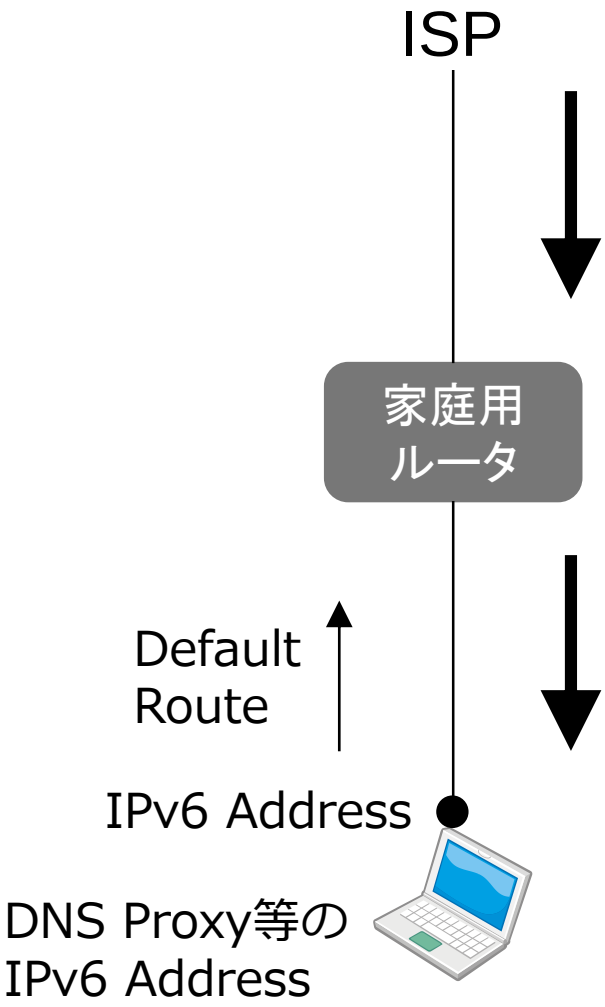


(IPv6)
家庭用ルータのLAN側
(ISPから見ると1ホップ先)
プレフィックス(アドレス群)



IPv6アドレス自動設定のためのプロトコル

端末に各種の情報を自動設定する。
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

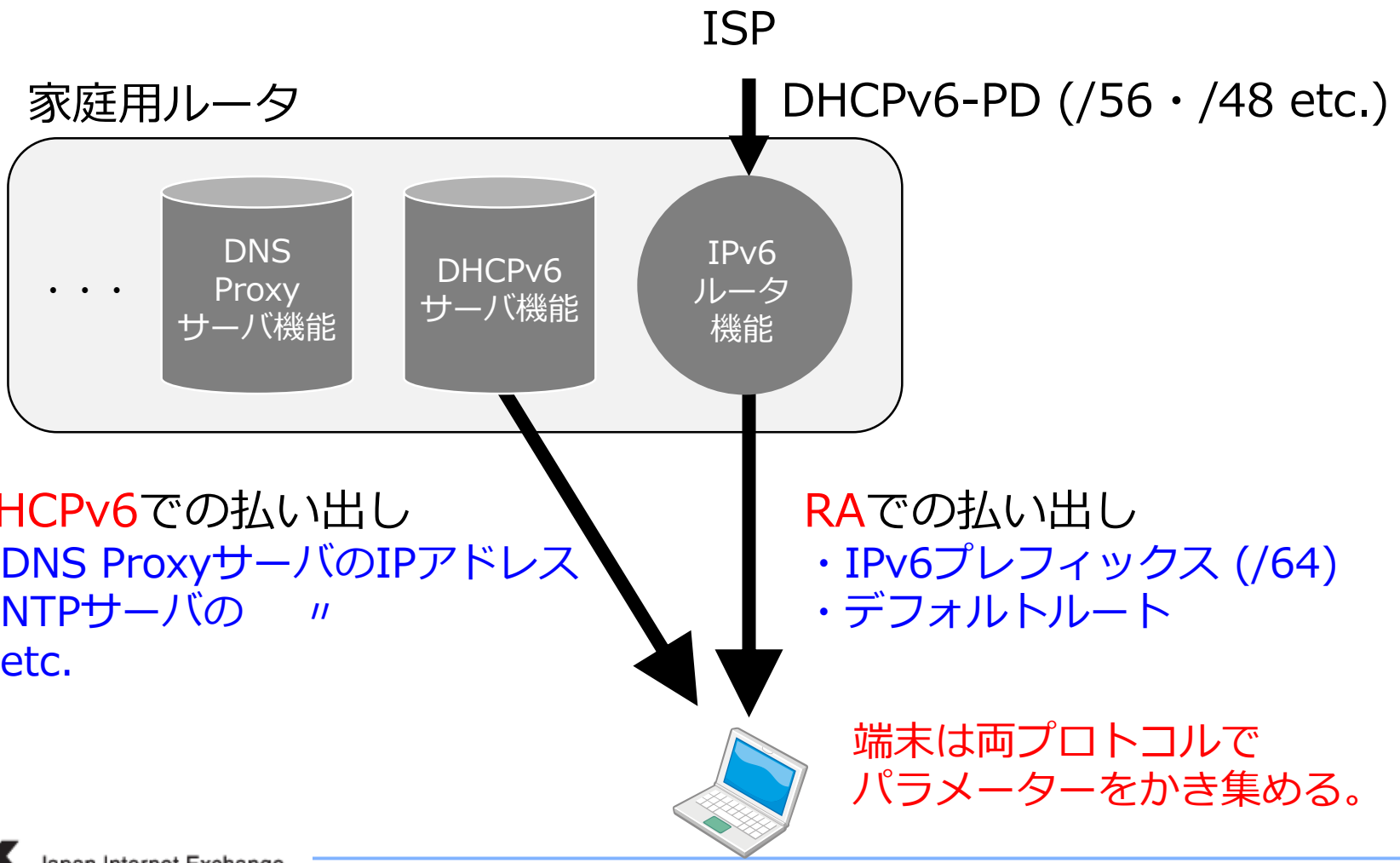
SLAAC方式(*1)
・RA　　(/64のPrefix・Default)
・DHCPv6　(DNSのIP 等)
を併用して自動設定

(例) 2001:0db8:1234:5678::/64

(*1) SLAAC：　Stateless Address Auto Configuration

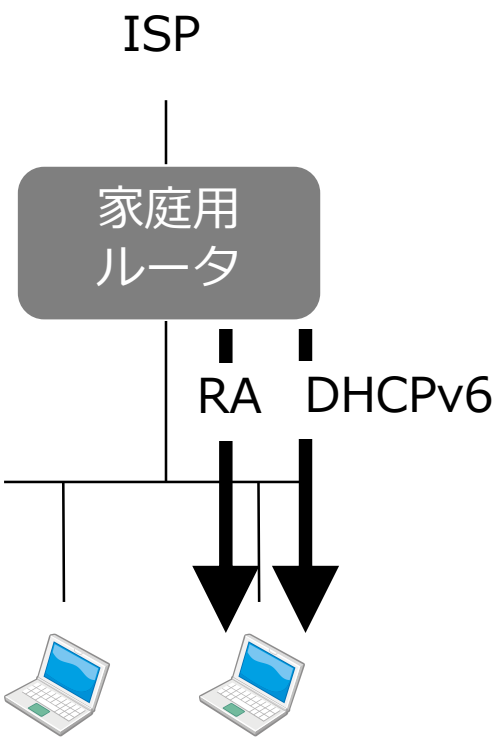
宅内アドレス等の設定動作例 (SLAACの例)

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はこれを使って。

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

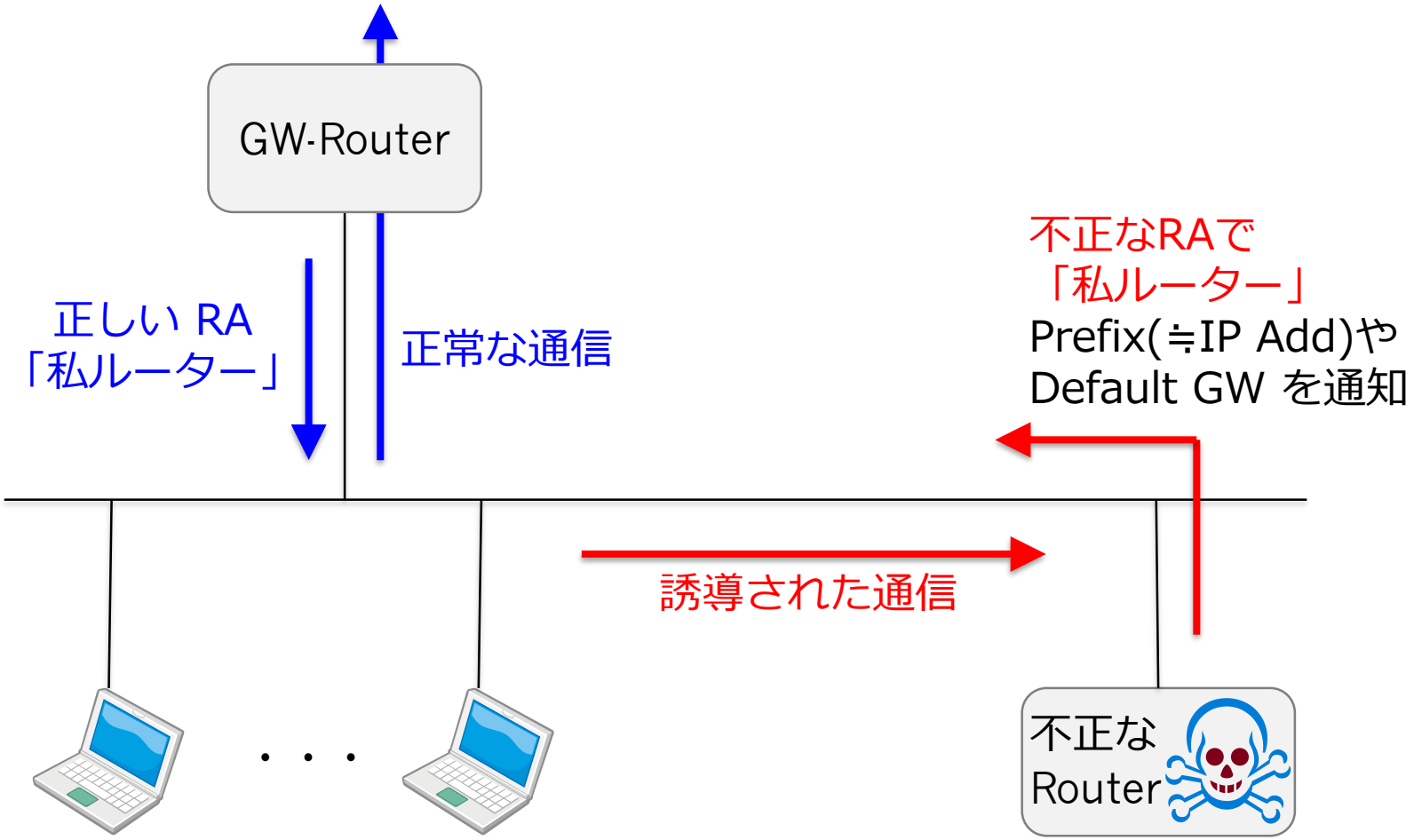
NDP
Neighbor Discovery Protocol

DHCPv6

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

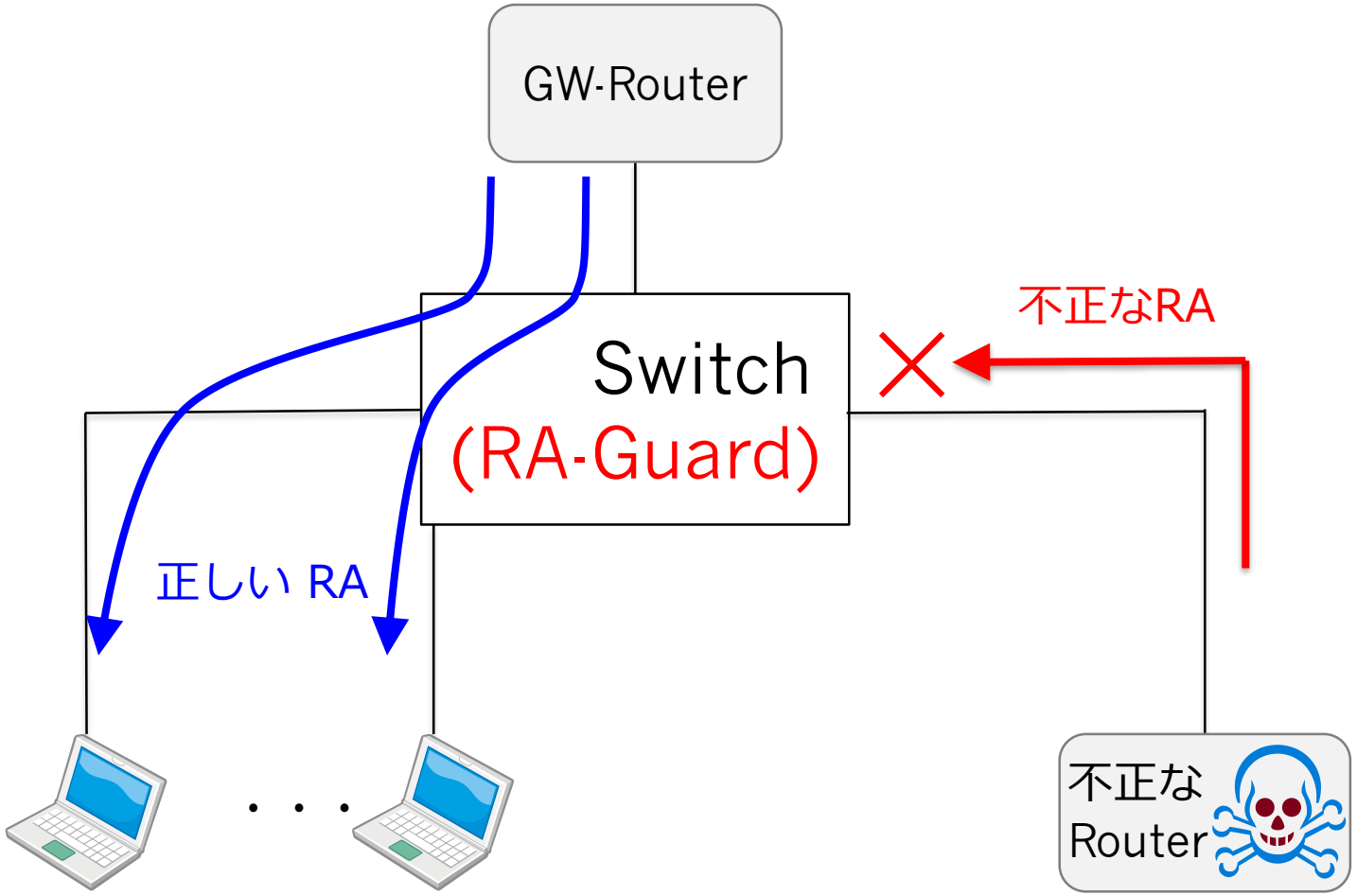
不正RA（Router Advertisement)

- 不正なRAにより、正常な通信ができなくなる。



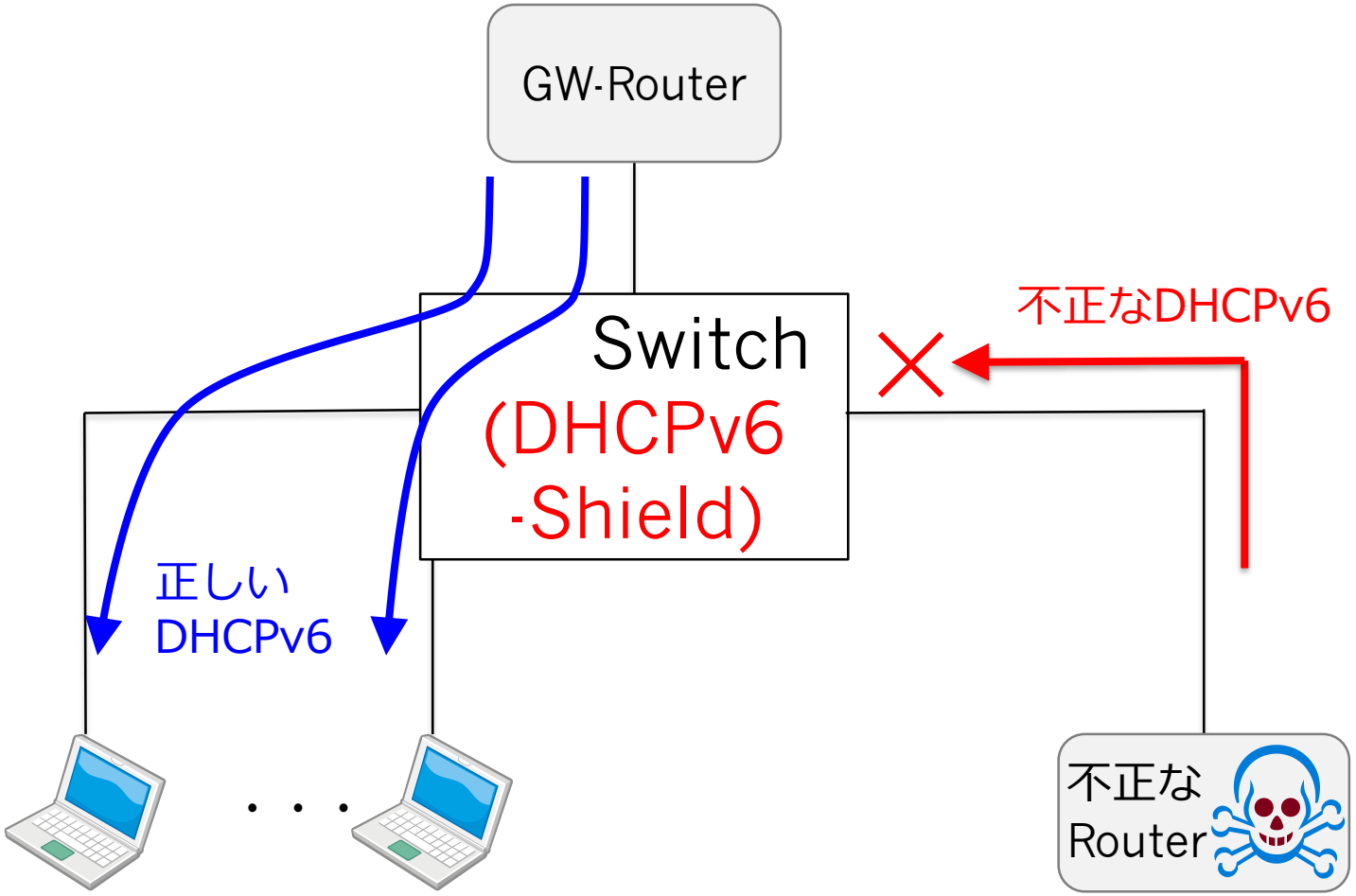
不正RAの対策例

- 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!



特記事項 (重要)

- 前述の「不正RA」や「不正DHCPv6」等は、IPv6 のイシューである。

- NW管理者が NW を IPv4-only としていても、最近の機器はデフォルトでIPv6が動いている。

IPv6 未対応の NW においても、
IPv6の問題が起きる可能性があることにご留意を !!

※ 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。

目次

- ウォーミングアップ
- IPv6セキュリティーのモチベーション
- LAN編
- **Home Router のフィルター編**
- プライバシー編
- ICMPv6編
- IPv4アドレス共有の影響編

(Home Router のフィルター編)

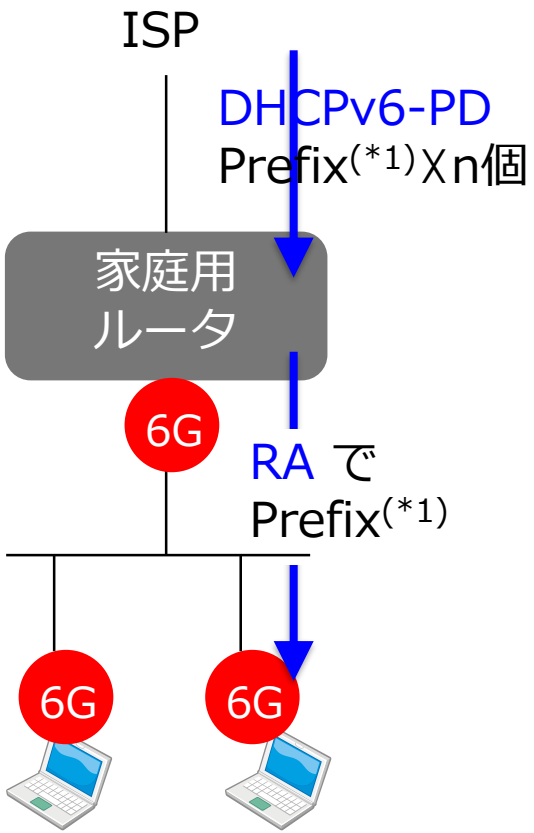
様々なIPv6アドレス自動設定

(筆者がどれを推奨するかは別として)

国内では、少なくとも3つの方式が使われている。

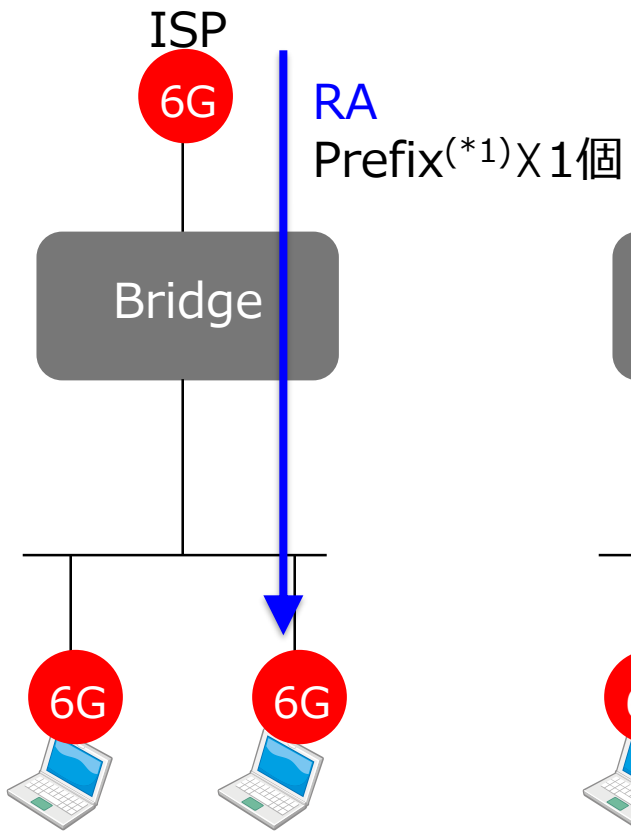
①家庭にルータを設置

世界で大多数



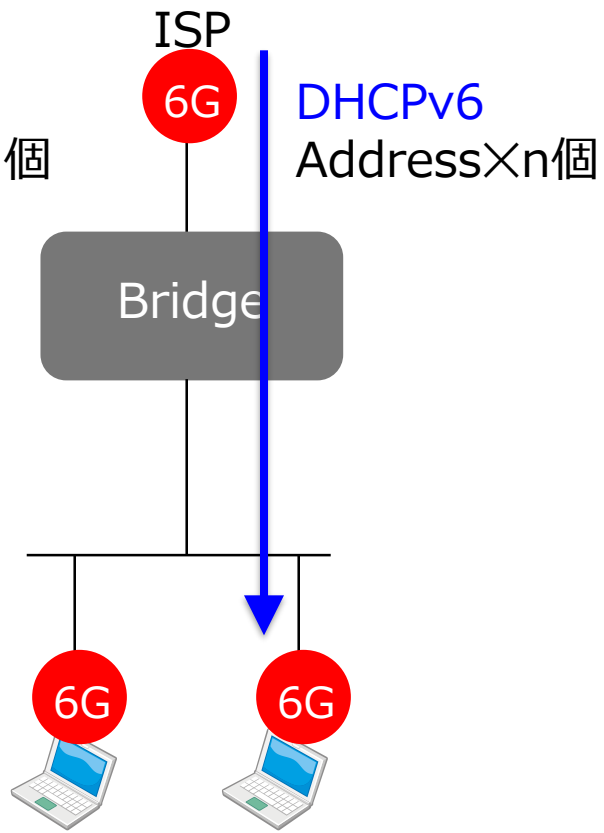
②局からRA

NGN光電話なし



③局からDHCPv6

一部のケーブル事業者

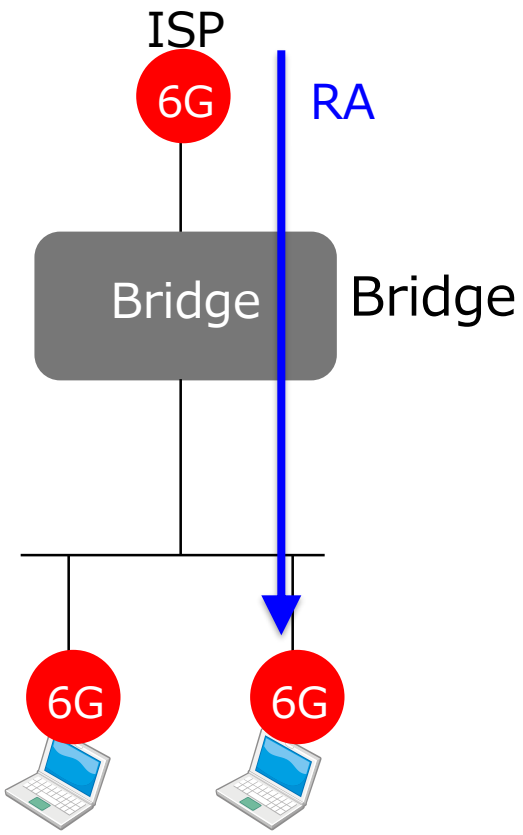


(*1) IPv6 Address が2の64乗個

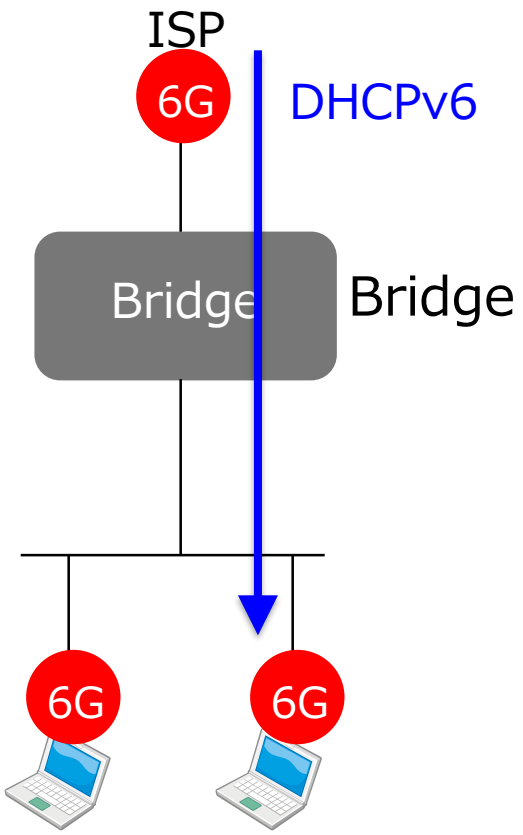
Home Router のフィルター

Bridge(L2)として動く Home Router にフィルター(L3)が実装されないことが有りがち。ご注意を。

局からRA



局からDHCPv6



インターネットからLANにアクセスできてしまう。

筆者の知る限り、少なくとも以下のメーカーの IPv4 over IPv6 (MAP-E/DS-Lite)対応機器は、フィルター対応済み

- IO-DATA
- Buffalo
- NEC

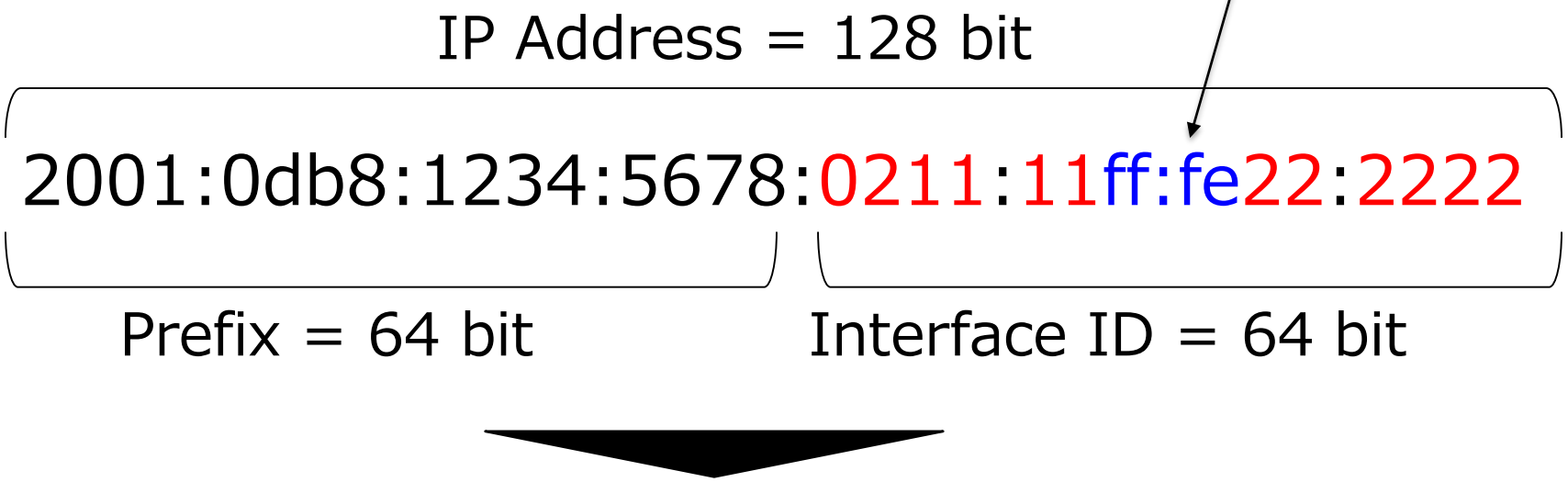
目次

- ウォーミングアップ
- IPv6セキュリティーのモチベーション
- LAN編
- Home Router のフィルター編
- **プライバシー編**
- ICMPv6編
- IPv4アドレス共有の影響編

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。

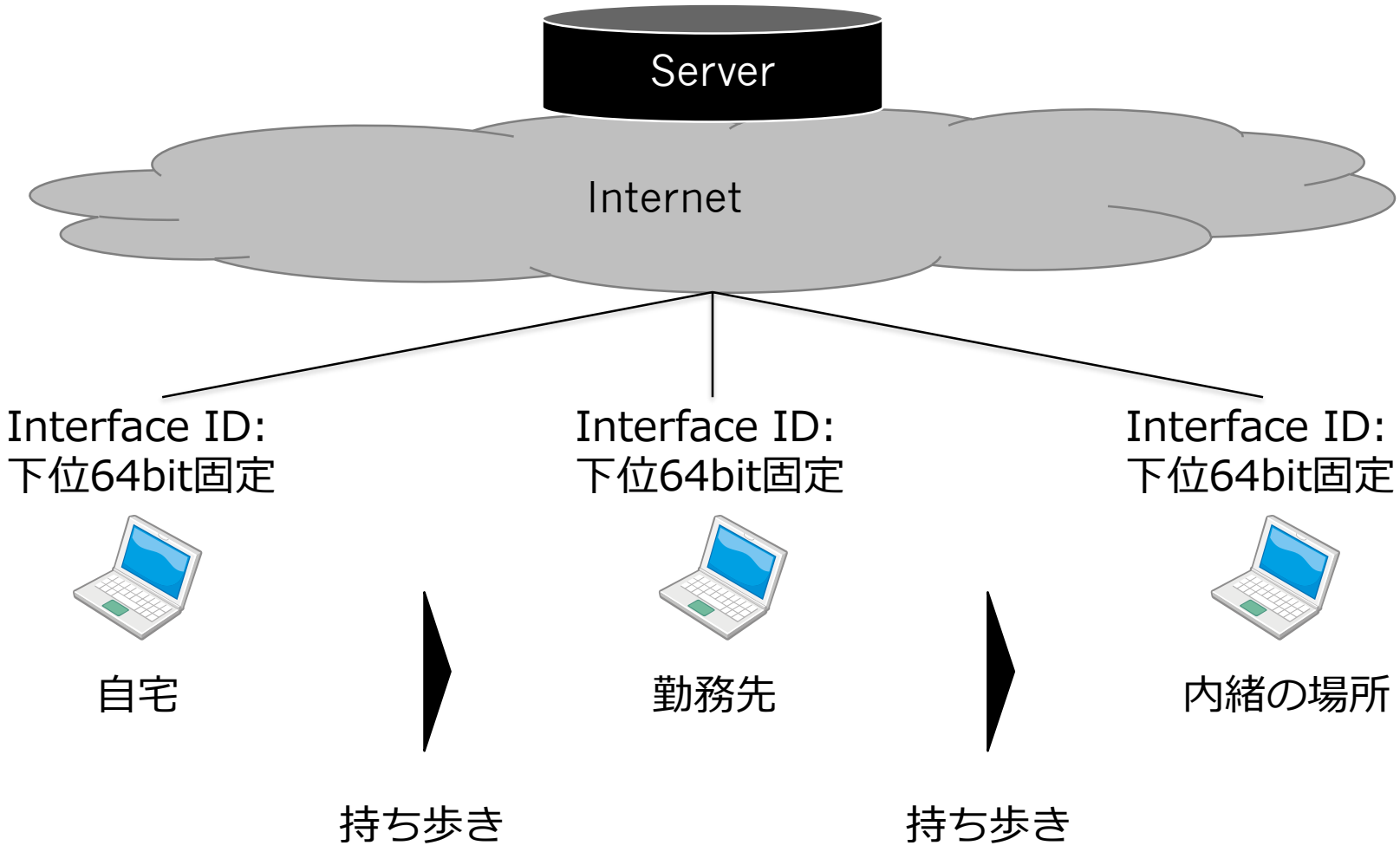
MACアドレスを2つに割って
真ん中に ff:fe を機械的に挿入



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。

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。



(プライバシー編)
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。

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アドレスプライバシー確保の手段

IPv6アドレス下位 64bit をランダムに生成する手段としていくつかのRFCが出ている。

- RFC3041 (廃止されてRFC4941へ)
  - Privacy Extensions for Address Configuration in IPv6
- RFC4941
  - Privacy Extensions for Stateless Address Autoconfiguration in IPv6
- RFC7217
  - A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)

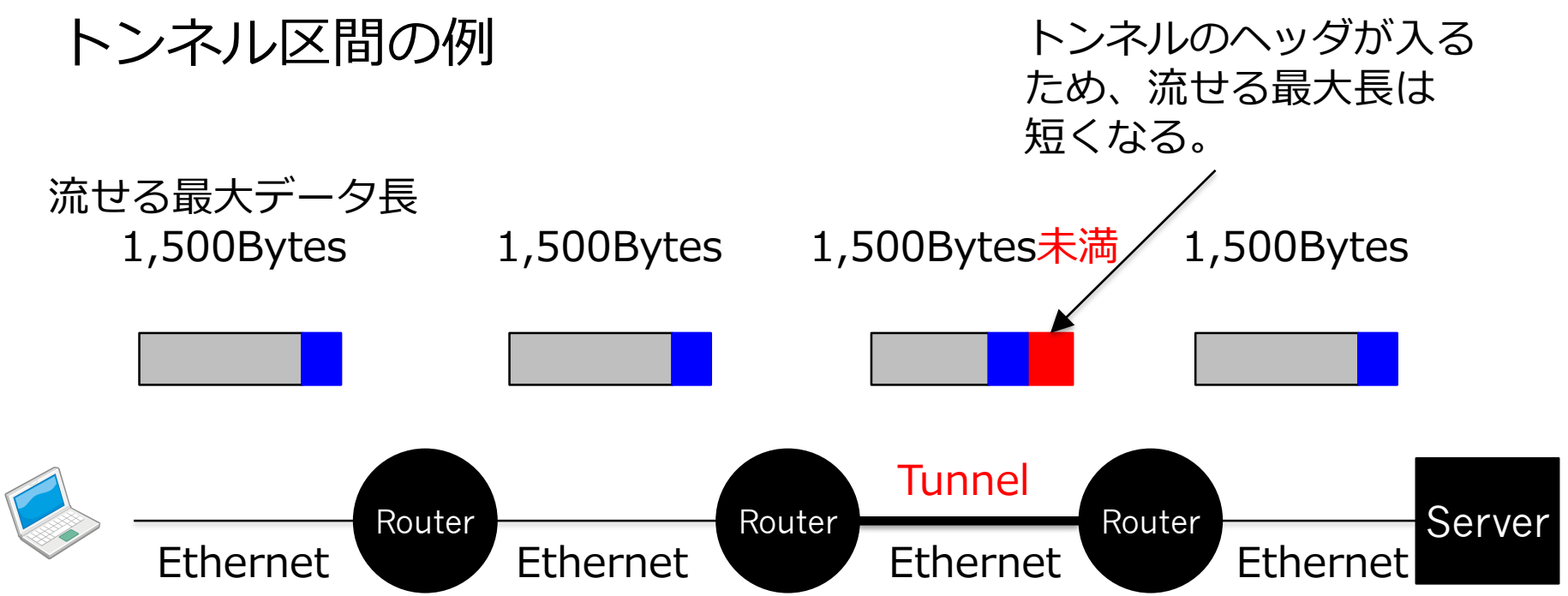
目次

- ウォーミングアップ
- IPv6セキュリティーのモチベーション
- LAN編
- Home Router のフィルター編
- プライバシー編
- **ICMPv6編**
- IPv4アドレス共有の影響編

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。

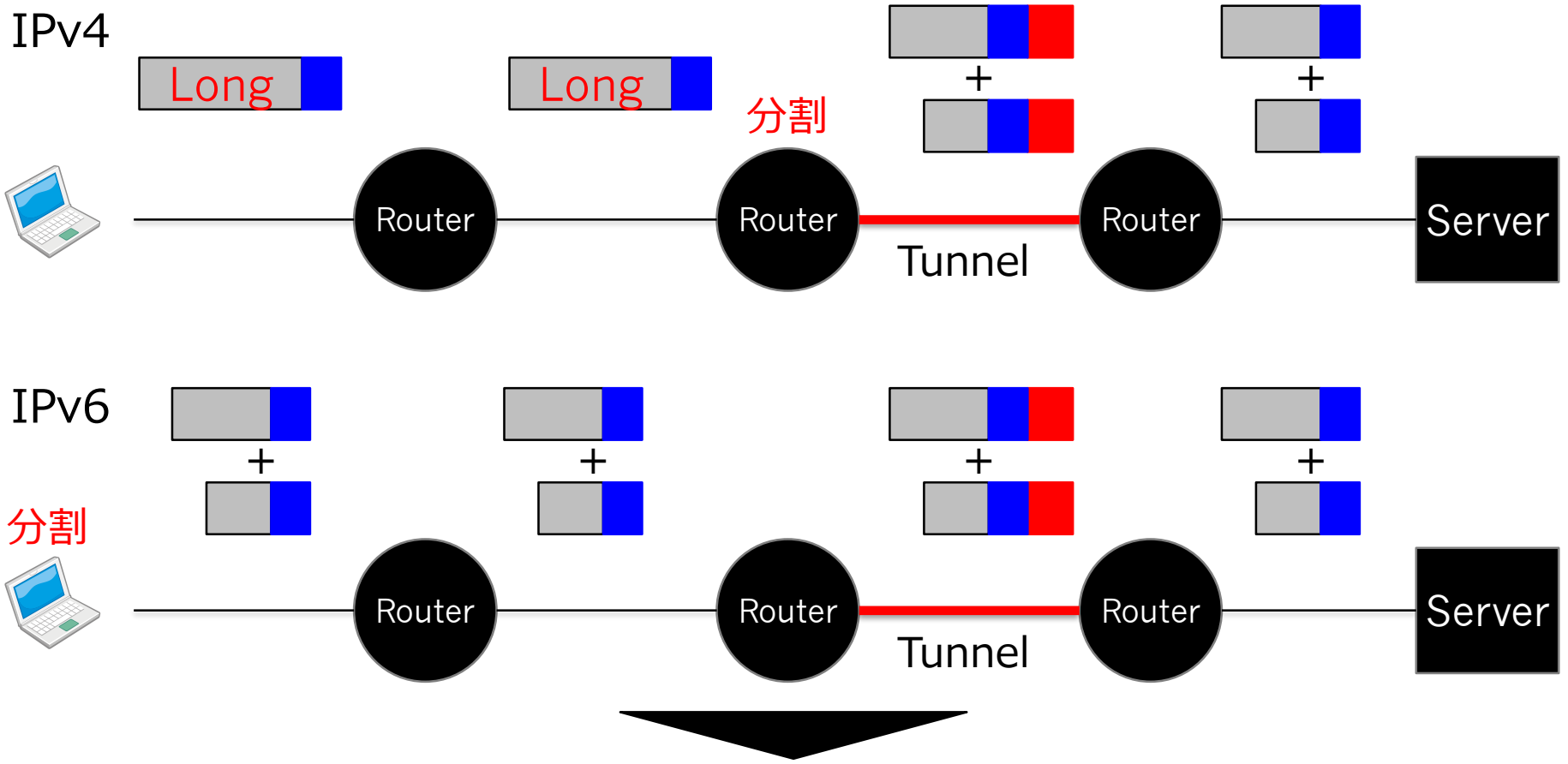
トンネル区間の例



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)

長いパケットを通す手段、IPv4 vs IPv6

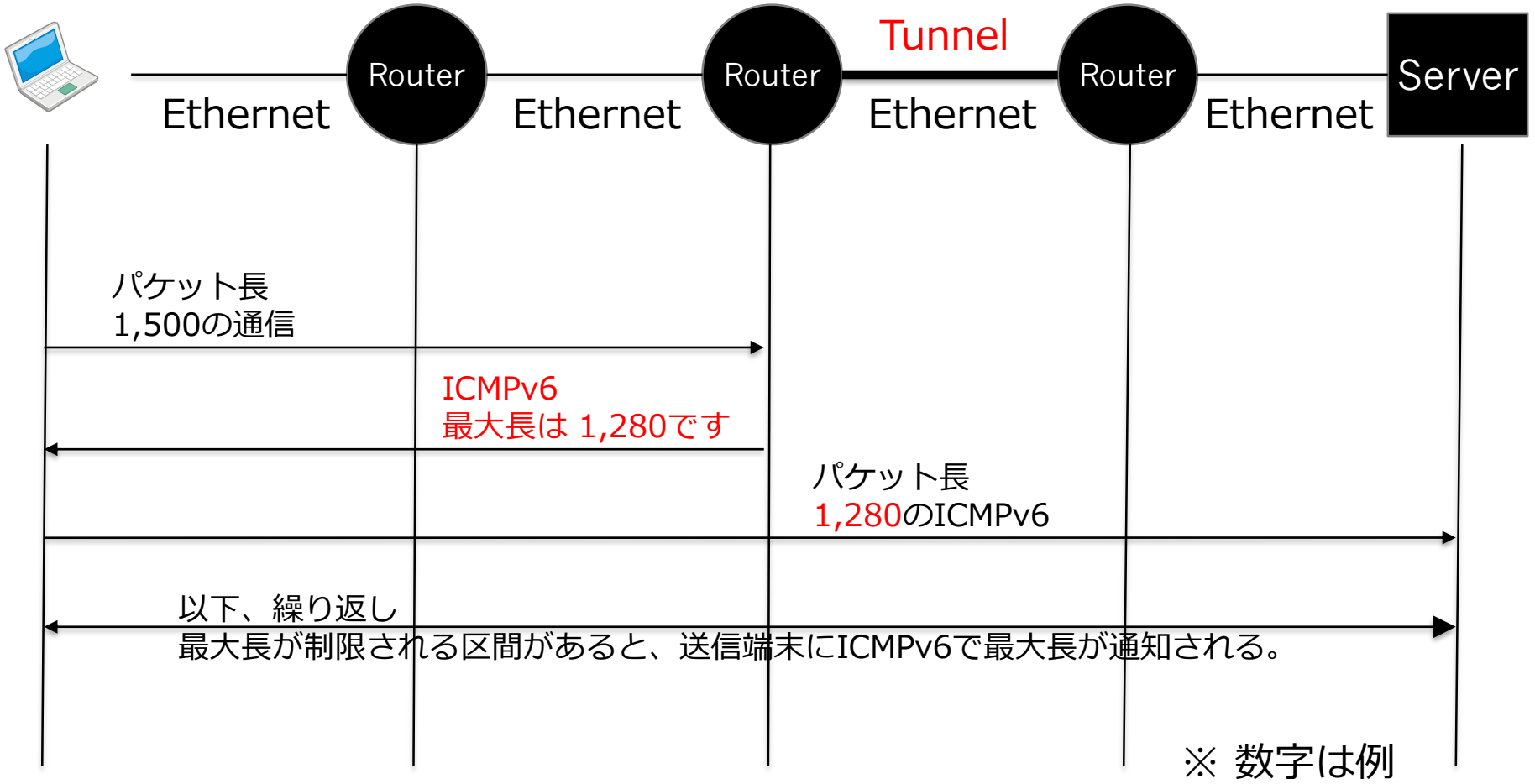
IPv4では、中継ルーターがパケットを分割(フラグメンテーション)していた。
IPv6では、送信端末が分割して送る。



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 とセキュリティーの関係は？

この ICMPv6 をフィルターアウトしてしまうと、ロングパケットが通らなくなる。→ 通信不可。

自組織に ICMPv6 をフィルターするべき、というセキュリティーの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。

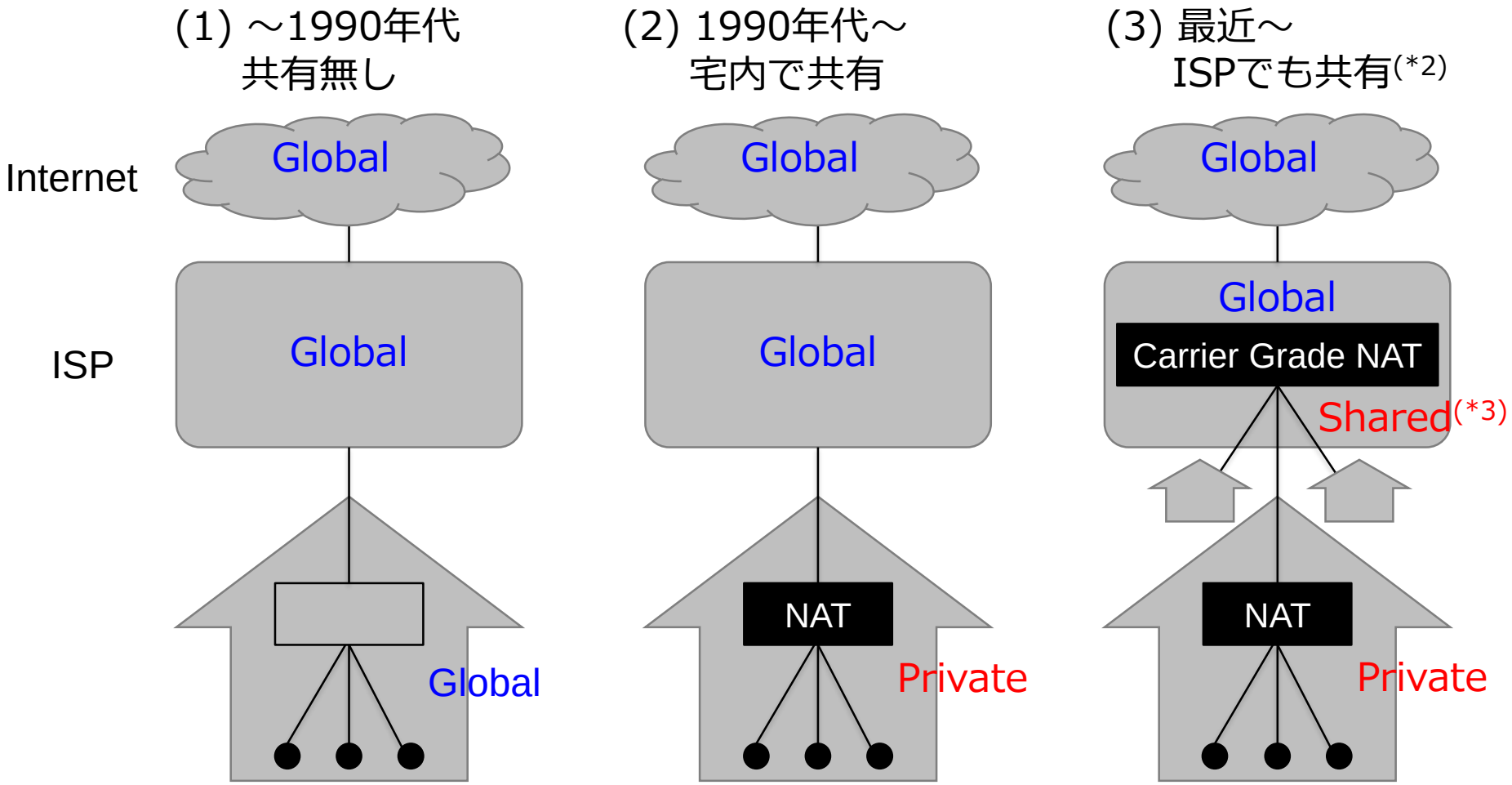
目次

- ウォーミングアップ
- IPv6セキュリティーのモチベーション
- LAN編
- Home Router のフィルター編
- プライバシー編
- ICMPv6編
- **IPv4アドレス共有の影響編**

(IPv4アドレス共有の影響)

アドレス共有が進む IPv4

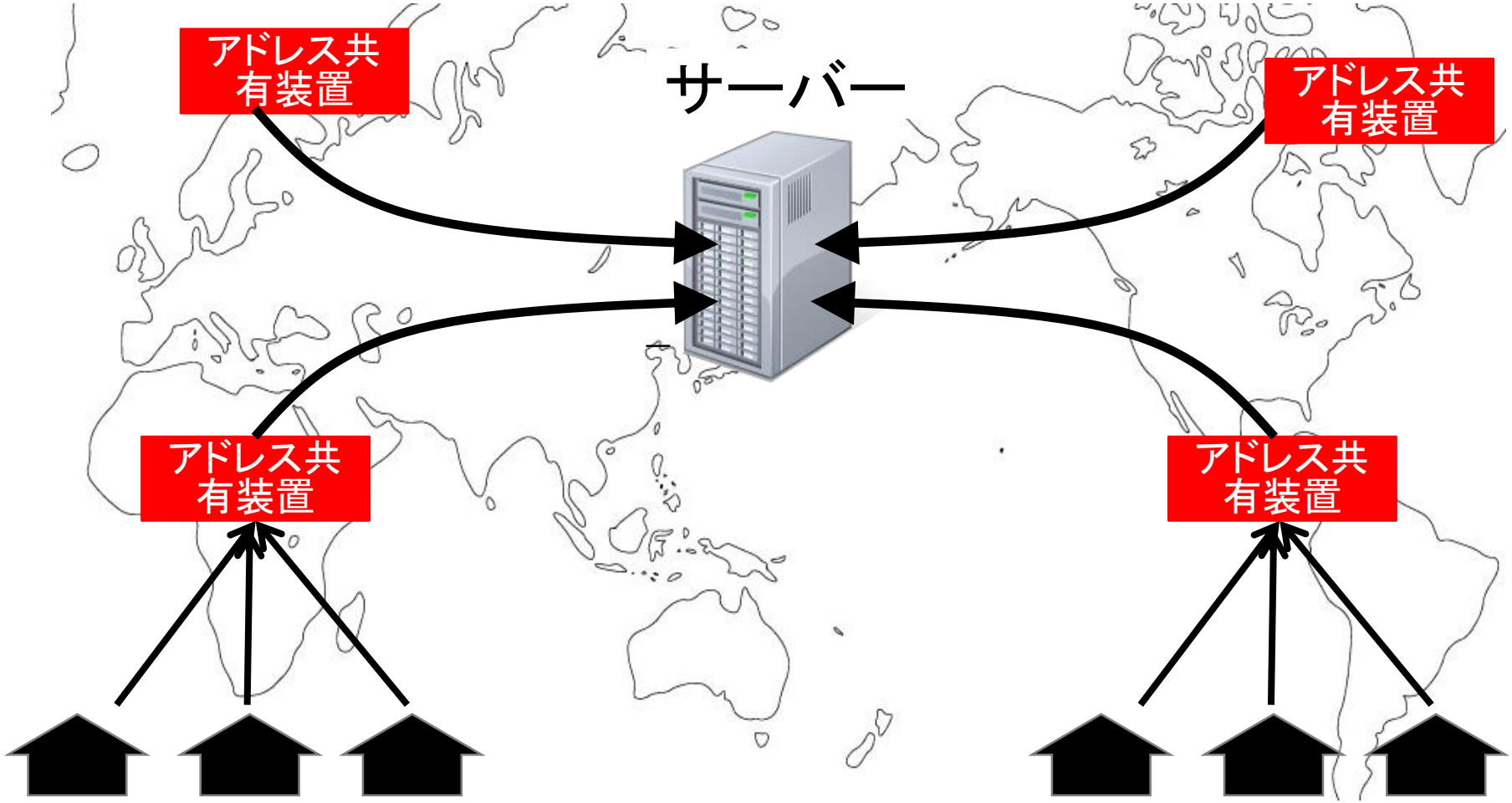
- 1つの IPv4 グローバルアドレスを複数で利用
- NAT(*1)等アドレス共有装置配下の各端末は IPアドレス+ポート番号で識別される。



(*1)正確にはNAPT。広義の「NAT」と言われることが多い。(*2) 方式は複数存在する。図は代表例
(*3)広義の「Private Address」と言われることが多いが、CGN用に「Shared Address空間」(RFC6598)が存在する。

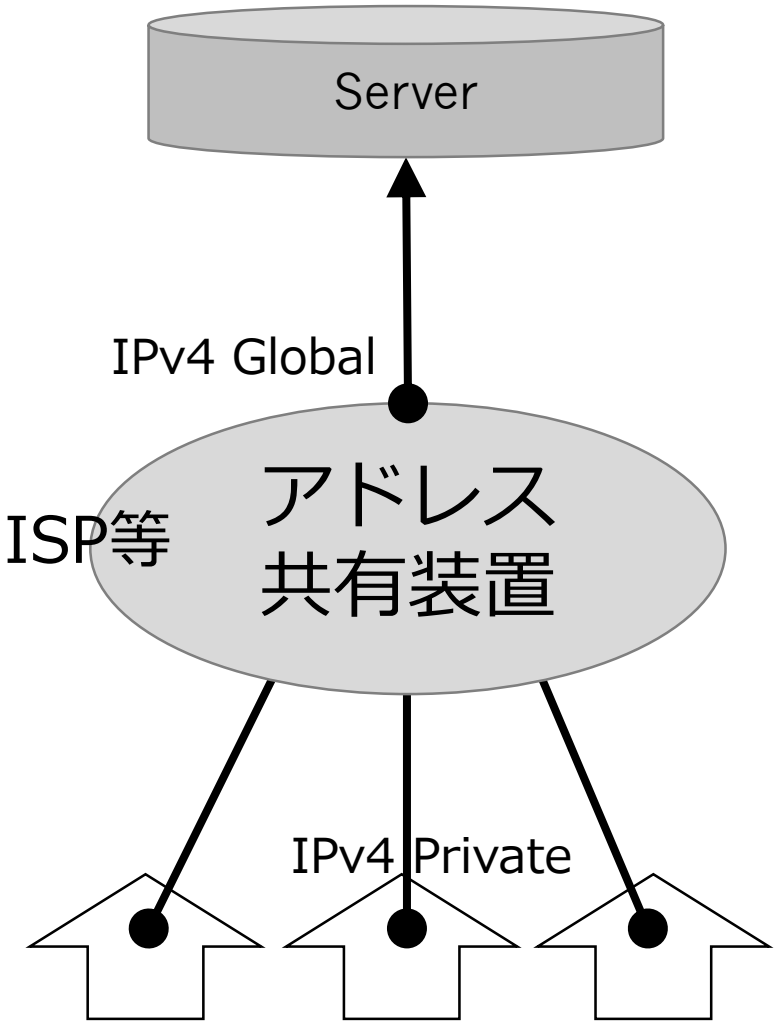
IPv4アドレス共有の導入状況

世界規模で「アドレス共有」が始まっている。



IPv4アドレス共有の影響

送信者のアドレスが同じため、送信者の特定が難しくなる。



影響例

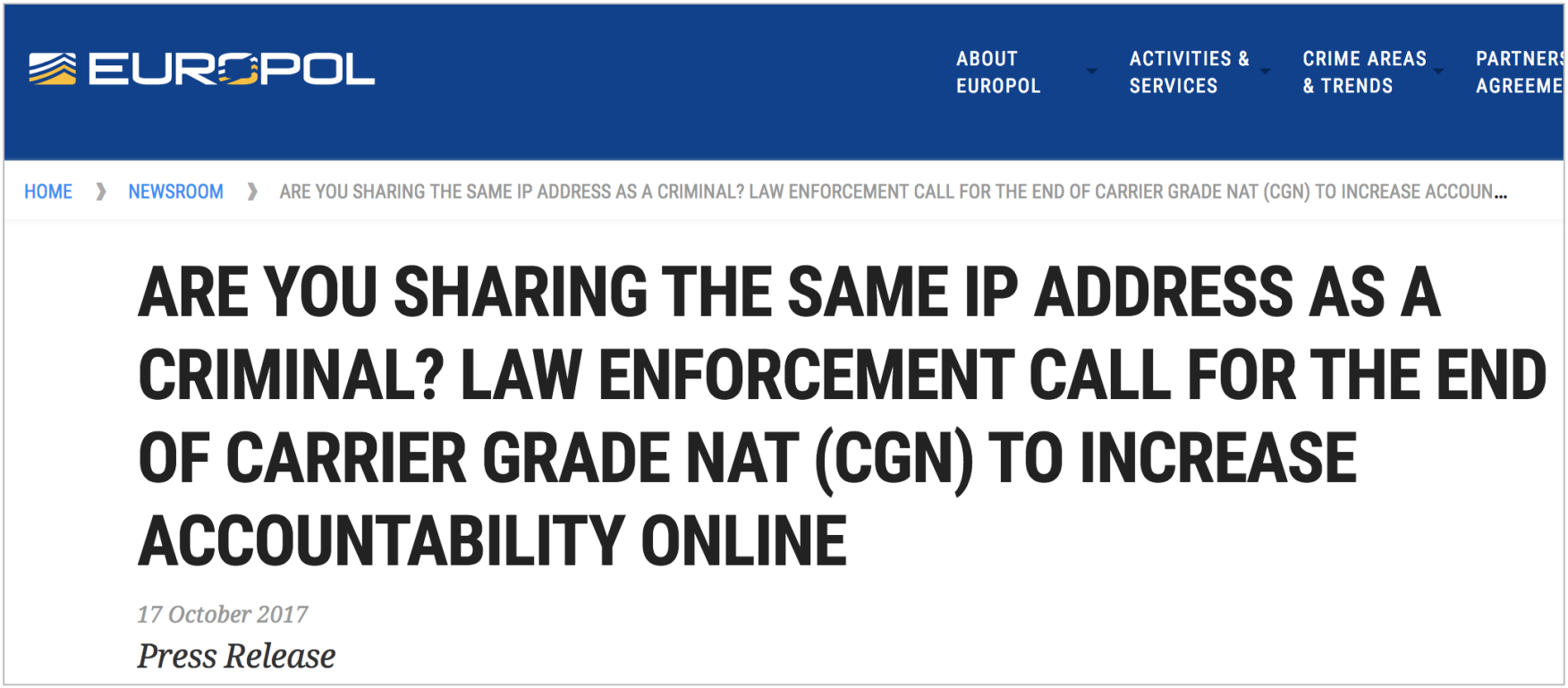
- 掲示板
  - 不正に書き込んだ人の特定が難
- DoS攻撃
  - 攻撃者の特定が難
- 犯罪捜査
  - 犯人の特定が難

(IPv4アドレス共有の影響)

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



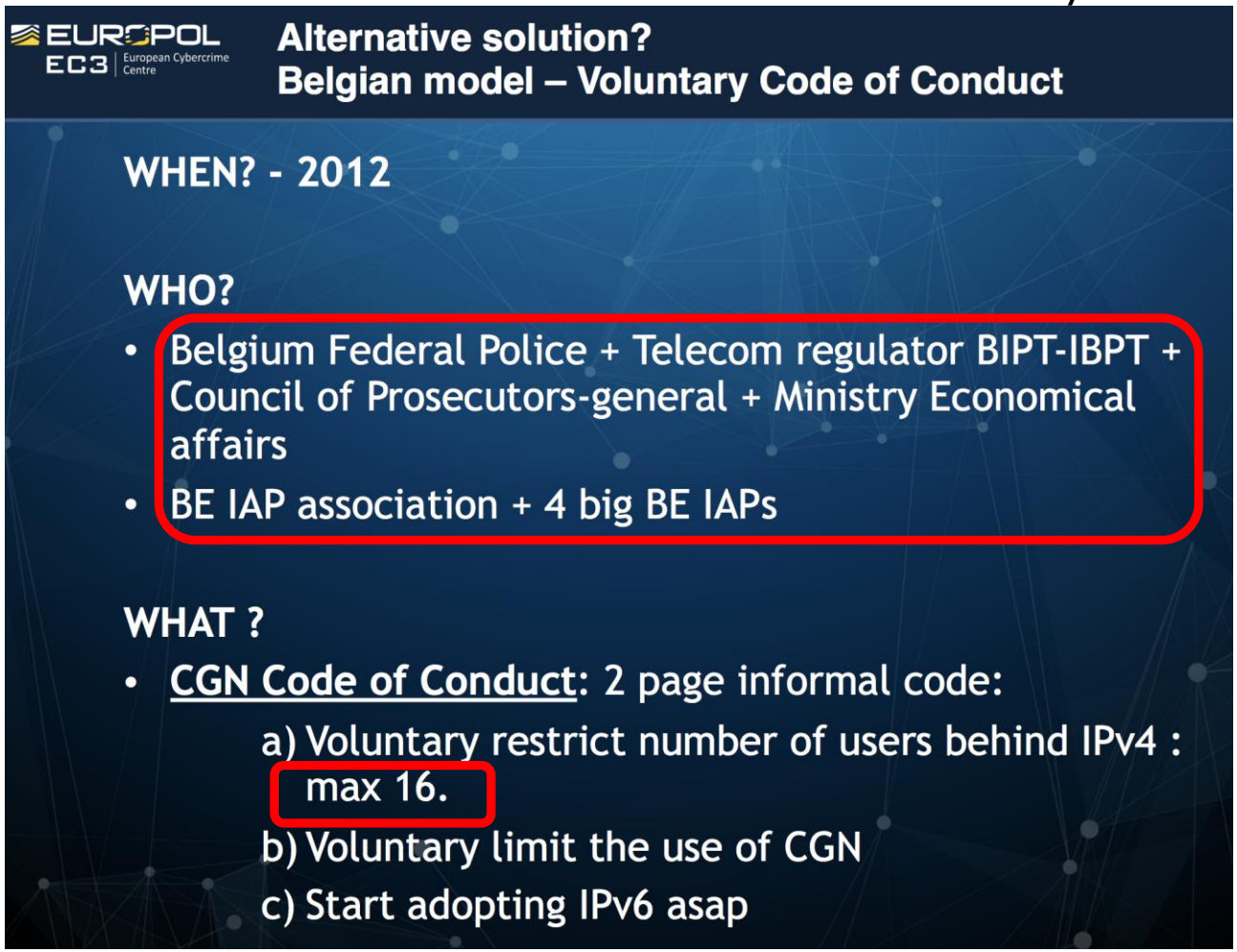
https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online

(IPv4アドレス共有の影響)

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

送信者を特定するためには？

受信側サーバーで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

NWのデザインによっては、受信側サーバーのみならず、Firewall、Load Balancer等での取得が必要となる場合がある。

- 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。

最後に

昨今の Internet には、思った以上にIPv6が導入されてます。

本日はIPv6に関するセキュリティーの一部をご紹介しました。

本セッションを機に、ご自身のネットワークを再点検してみてはいかがでしょうか。


jpix