Innovative R&D by NTT

必修・IPv6セキュリティ
～未対応で大丈夫ですか？～

NTT ネットワーク基盤技術研究所
藤崎 智宏

IPv6の普及状況と
セキュリティ対策の必要性

IPv6の普及状況

概況

- 世界的に，IPv4のアドレス在庫不足が深刻化，IPv6普及に拍車がかかっている.

IPv4アドレスの在庫状況

http://www.potaroo.net/tools/ipv4/のデータより作成（2017.11.14）

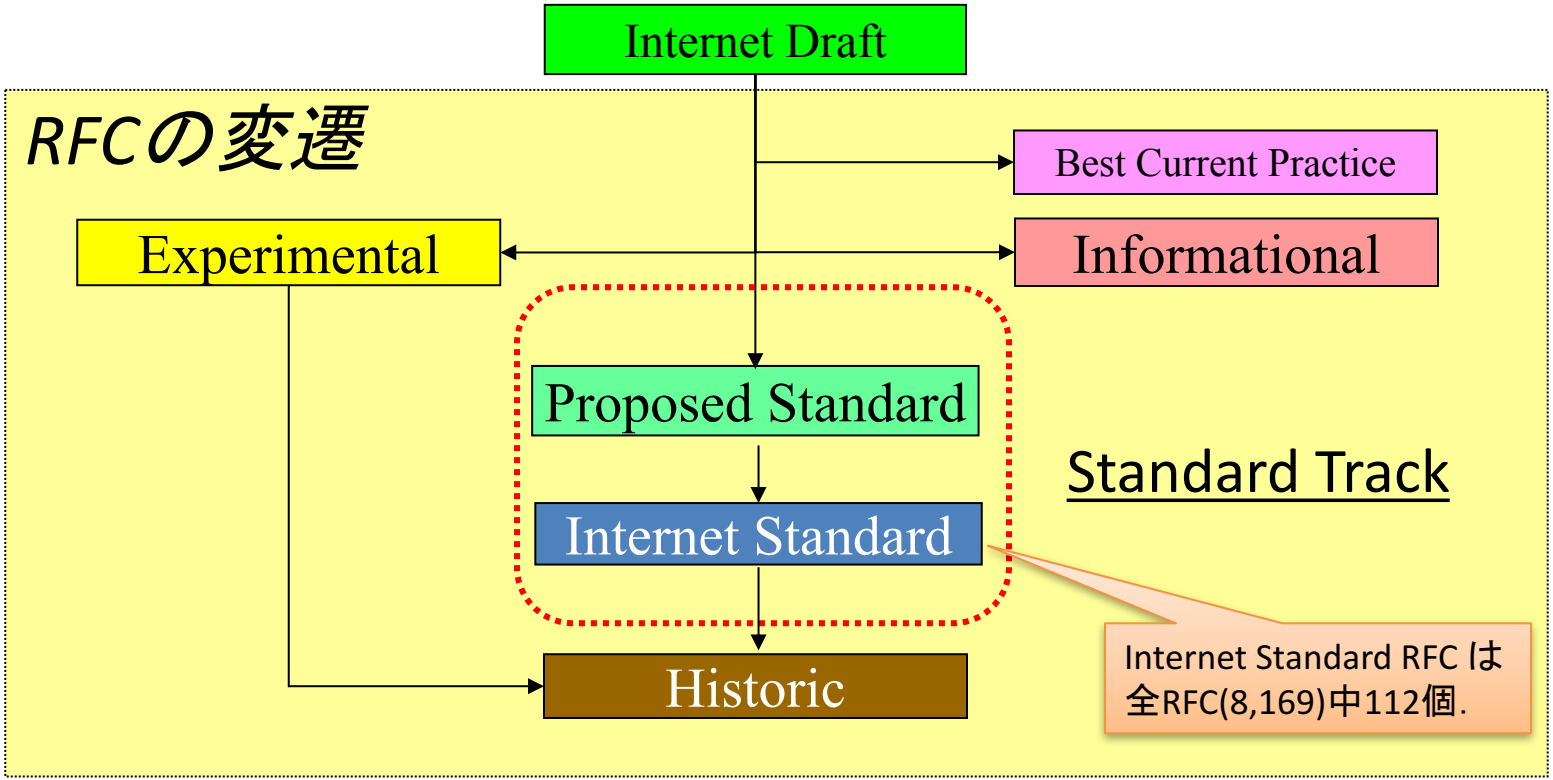
IPv6の普及状況

概況

- 世界的に，IPv4のアドレス在庫不足が深刻化，IPv6普及に拍車がかかっている.
- 2017年は，国内外的にIPv6的に大きなマイルストーンとなった年
  - IPv6標準仕様が”インターネット標準”となる.
  - 国内大手携帯三社が，IPv6サービスを本格的に開始
  - 国内大手ISPのIPv6対応が進展

IPv6標準仕様の”インターネット標準”化

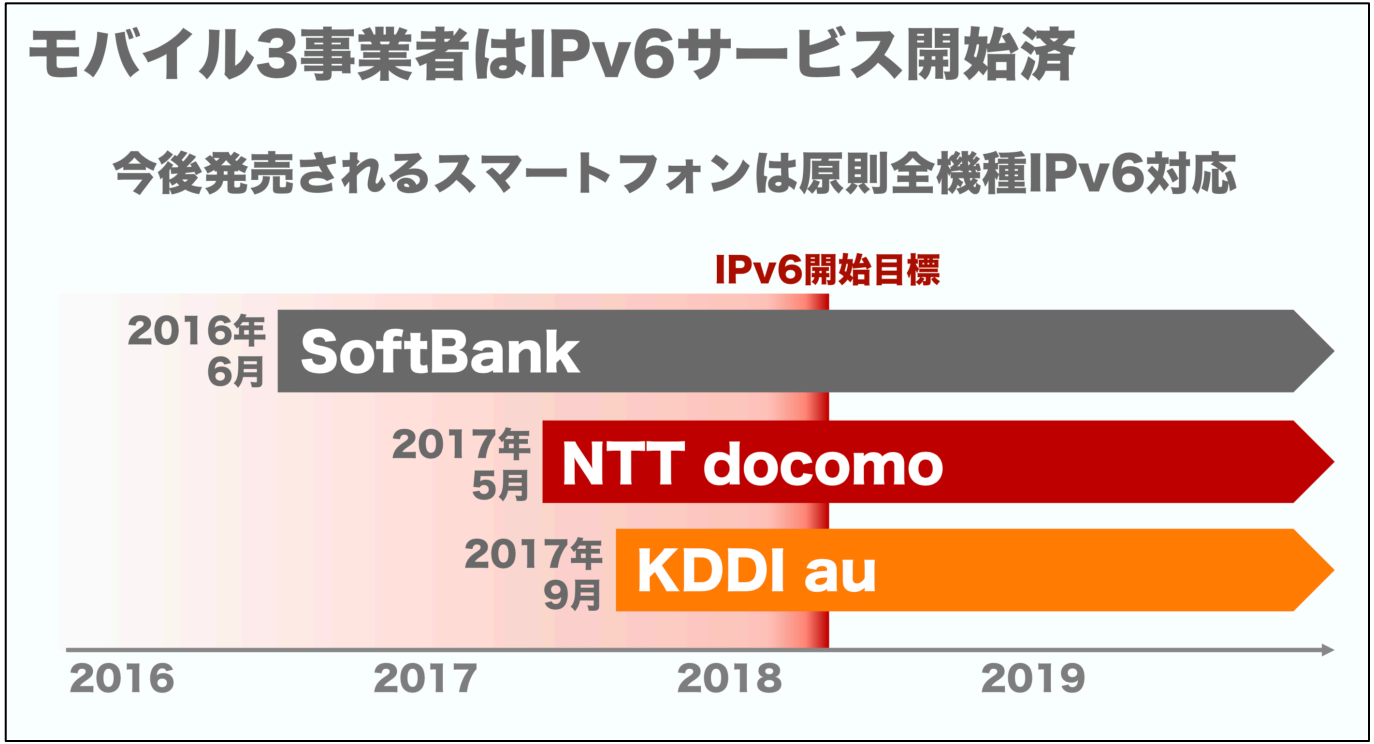
IETFにおける標準化プロセス



IPv6標準仕様の”インターネット標準”化

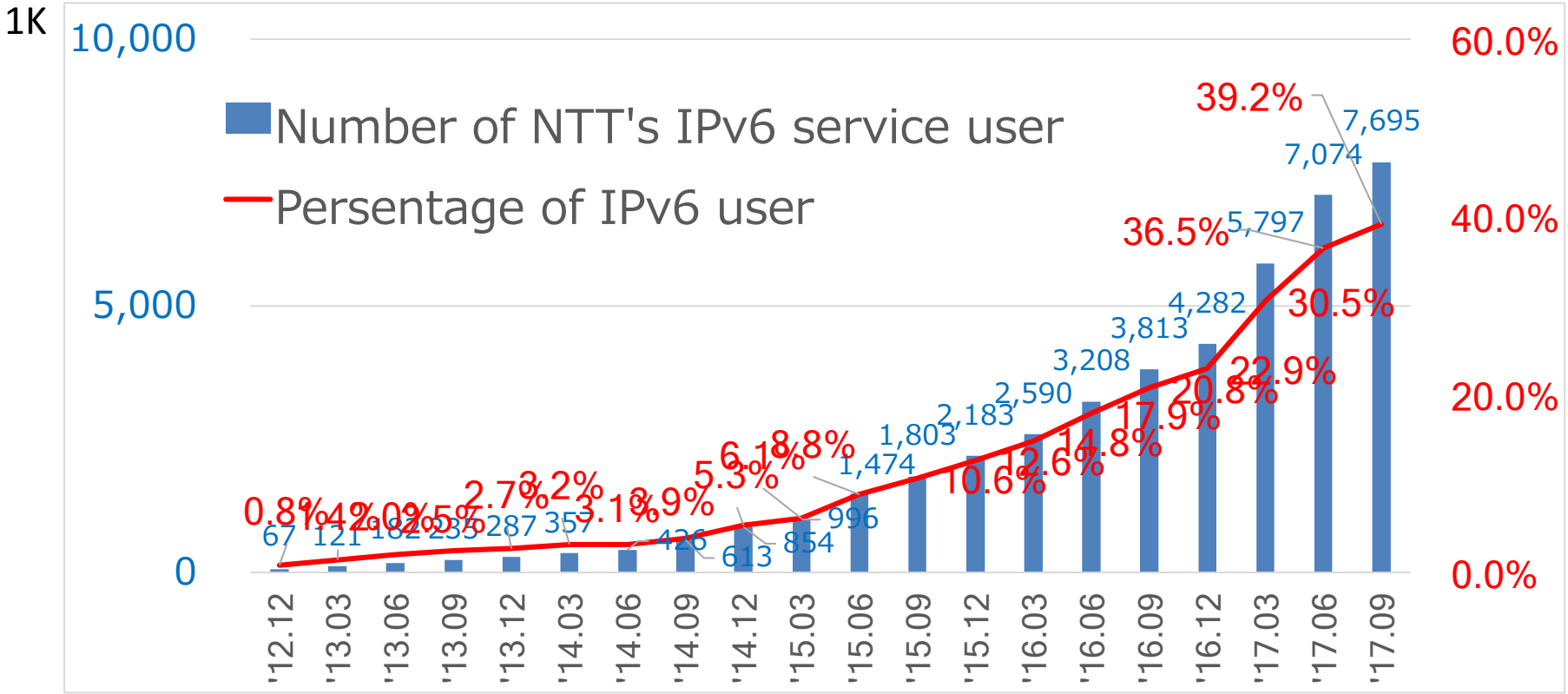
- IPv6の仕様が最高段階の標準に
  - STD0086: Internet Protocol, Version 6 (IPv6) Specification (RFC 8200)
  - STD0087: Path MTU Discovery for IP version 6 (RFC 8201)
  - STD0088: DNS Extensions to Support IP Version 6 (RFC3596)
  - STD0089: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (RFC4443)

携帯キャリアのIPv6対応状況



総務省「第36回IPv6によるインターネットの利用高度化に関する研究会」資料より抜粋

国内固定系ISPのIPv6導入状況 ～フレッツから～

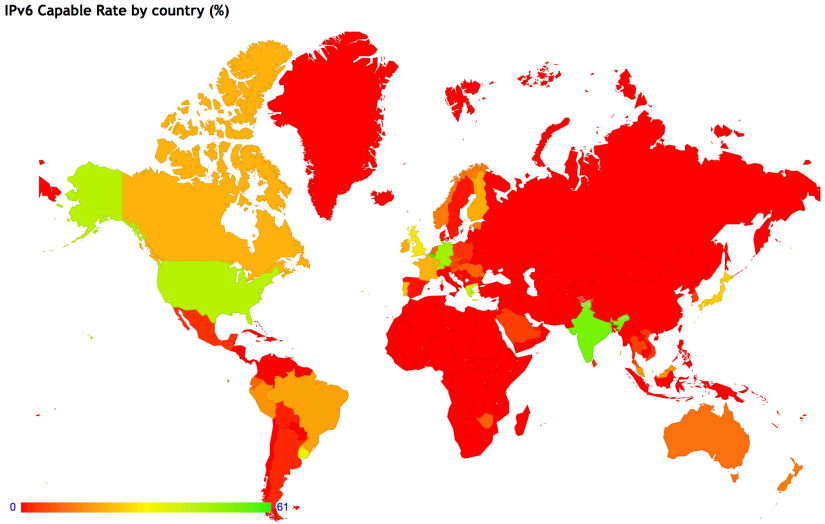


http://v6pc.jp/jp/spread/ipv6spread_03.phtml のデータより作成（2017.11.14）

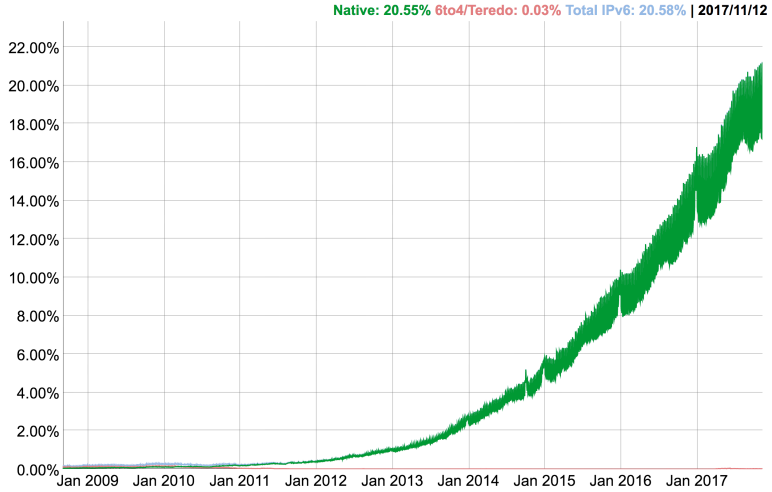
IPv6の世界的な状況

世界的に普及が進んでいます.

2017年11月14日現在



IPv6の普及度
https://stats.labs.apnic.net/ipv6/



Google サーバへの通信の割合
https://www.google.com/intl/ja/ipv6/statistics.html

機器の状況

- 多くの機器は，IPv6対応済み
  - スマートフォン，PC
  - ネットワーク機器（ルータ等）
- ディフォルトでIPv6が動作するようになっているものが多い

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

- 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

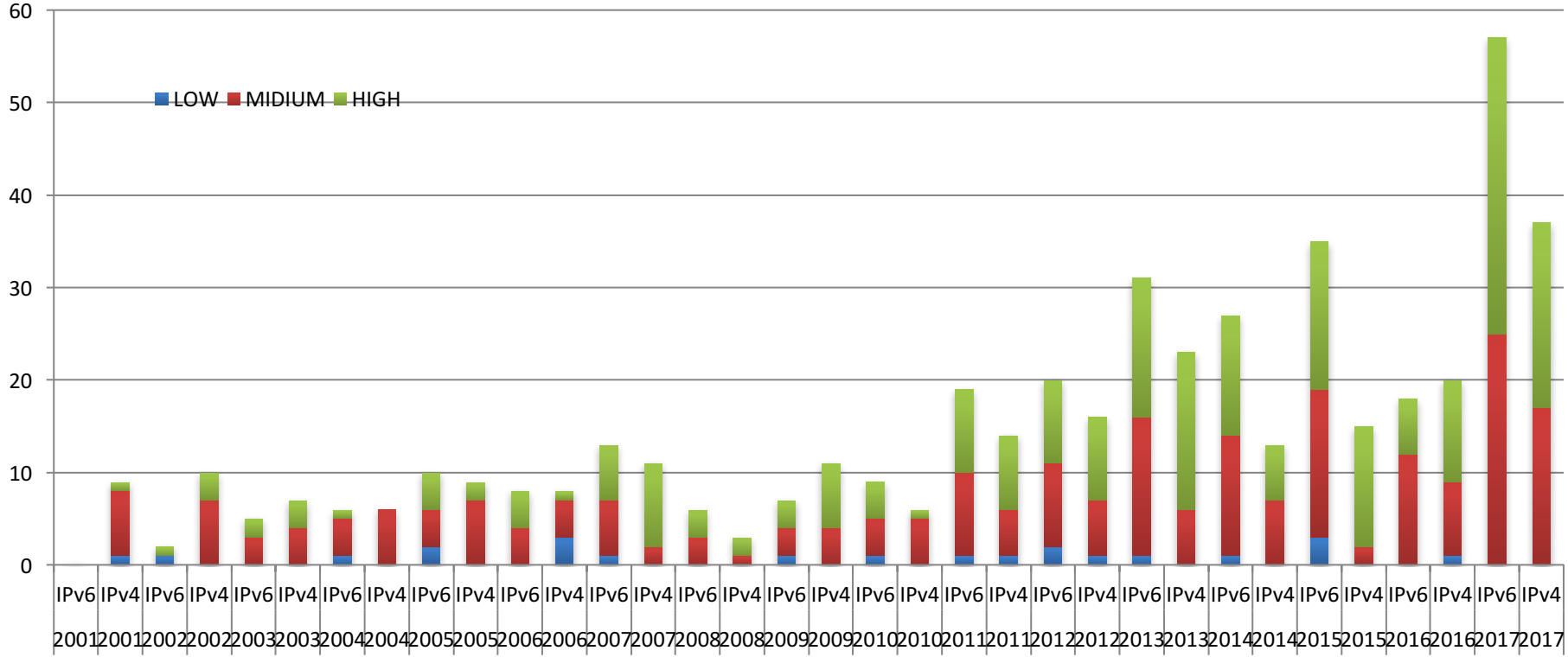
  - IPv6が広く利用されるようになって来た

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

IPv6に関するセキュリティ報告申告件数

脆弱性情報データベースCVEからのデータ（2017.11．13現在）

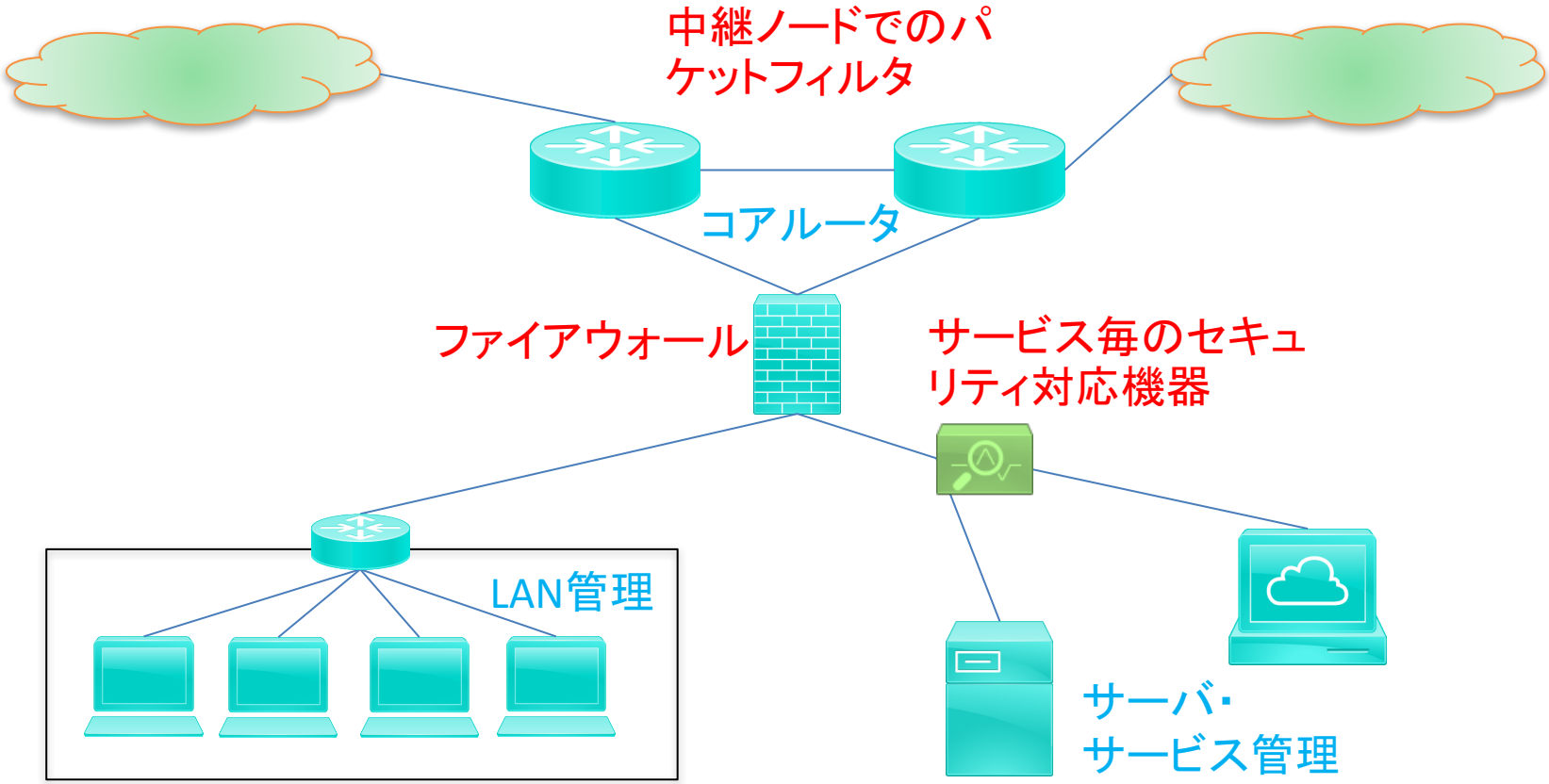


IPv6セキュリティ概説 -運用編-

IPv6におけるセキュリティ

- ”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

ネットワークのセキュリティ



- 運用する立場より，”セキュリティ” の観点から見た，IPv6とIPv4の違い
  - ICMPv6 と ICMP 【ファイアウォールの設定】
  - ND（Neighbor Discovery）と ARP【LAN管理】
  - アドレス種別，割当方法【IPv6アドレス管理】
    - リンクローカルアドレスの扱い
    - 使用するアドレスの選択
  - ルータ・ルーティングに関わるセキュリティ【ルータ管理】

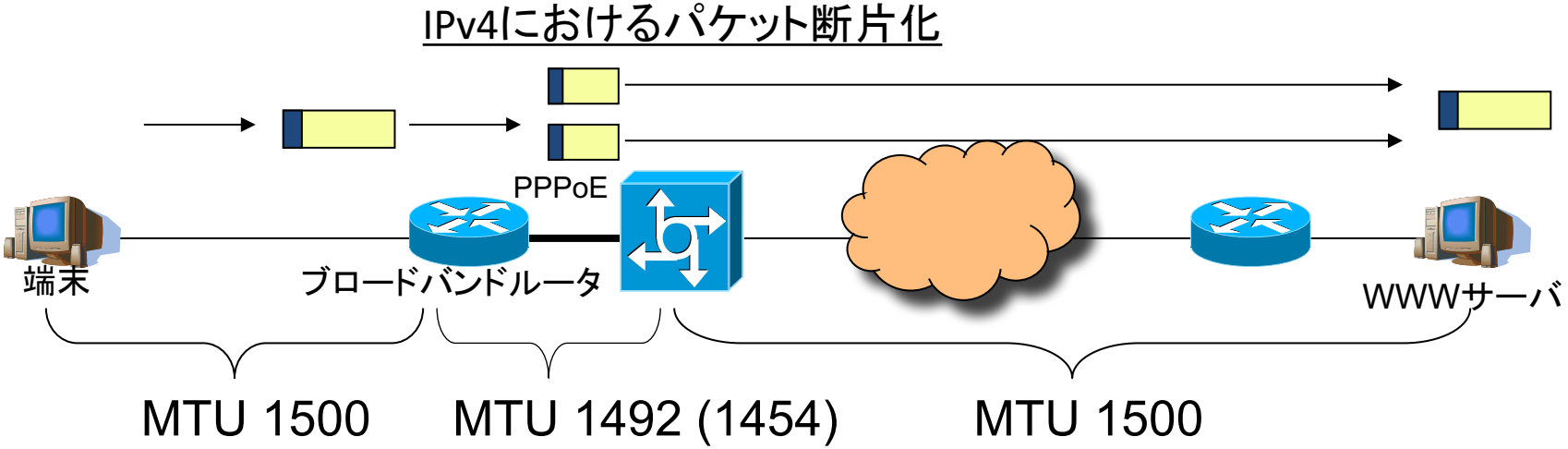
ファイアウォール関連

IPv6におけるファイアウォールの設定

- IPv4 と基本的な考え方は同じだが，ICMPv6の重要性に留意
  - IPv6では，通信に重要な役割を果たすパスMTU探索（PMTUD: Path MTU Discovery）に ICMPv6 を利用している.
    - IPv4でのICMPのフィルタポリシによっては，要注意
- IPv6の特徴の一つである，「拡張ヘッダ」の扱い

IPとパケット断片化（フラグメンテーション）

- IPでは，途中の経路で，転送可能なパケット最大長（MTU: Maximum Transmission Unit）が変わることがある
  - IPv4では，経路途中でパケットの断片化が発生

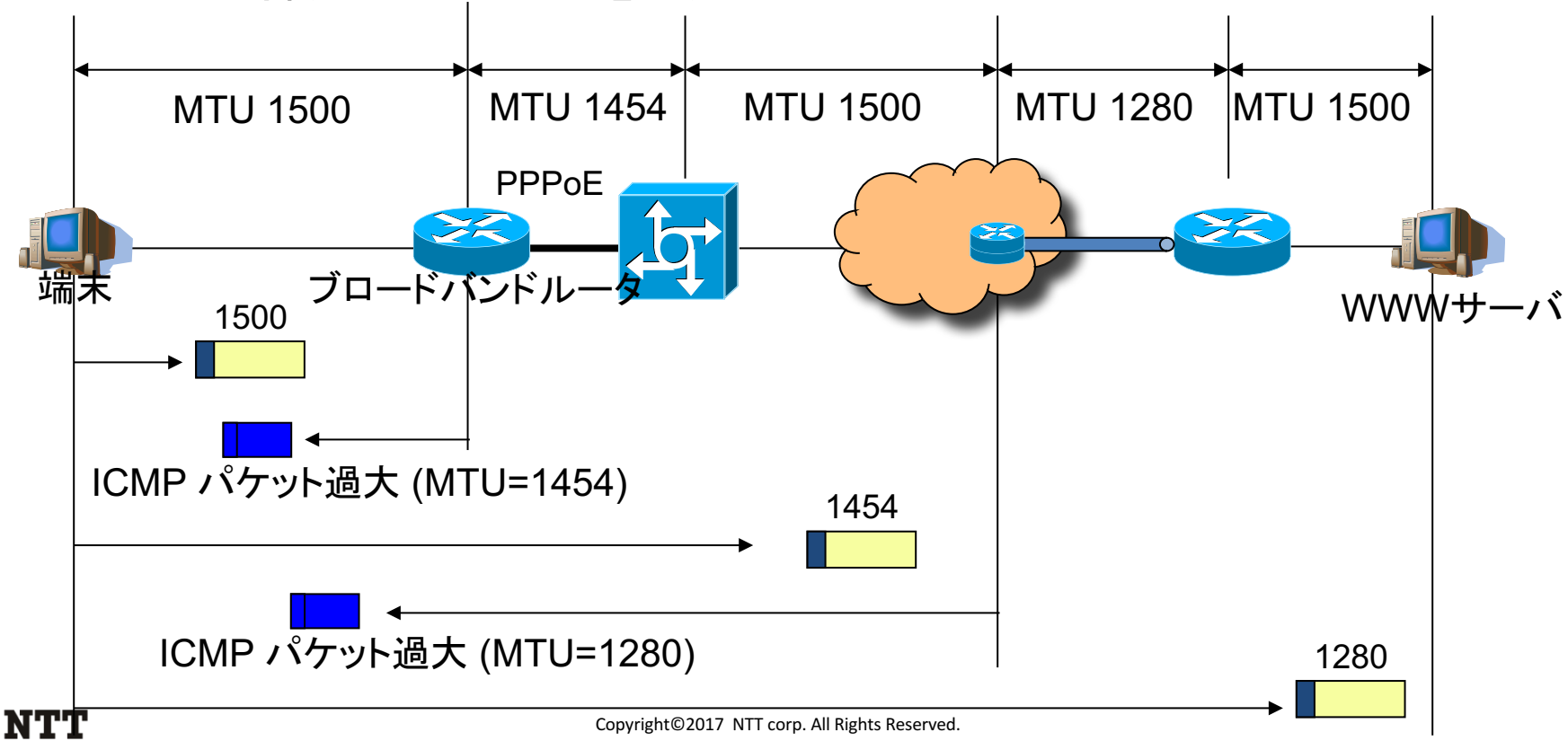


IPv6におけるパスMTU探索

- IPv6では経路途中の断片化はしない．断片化は，ソースノードが実施．
  - パケットは，通信相手までのMTUにて実施．パスMTU探索が重要な役割を占める．

IPv6におけるパスMTU探索

- パスMTU探索にはICMPv6を利用

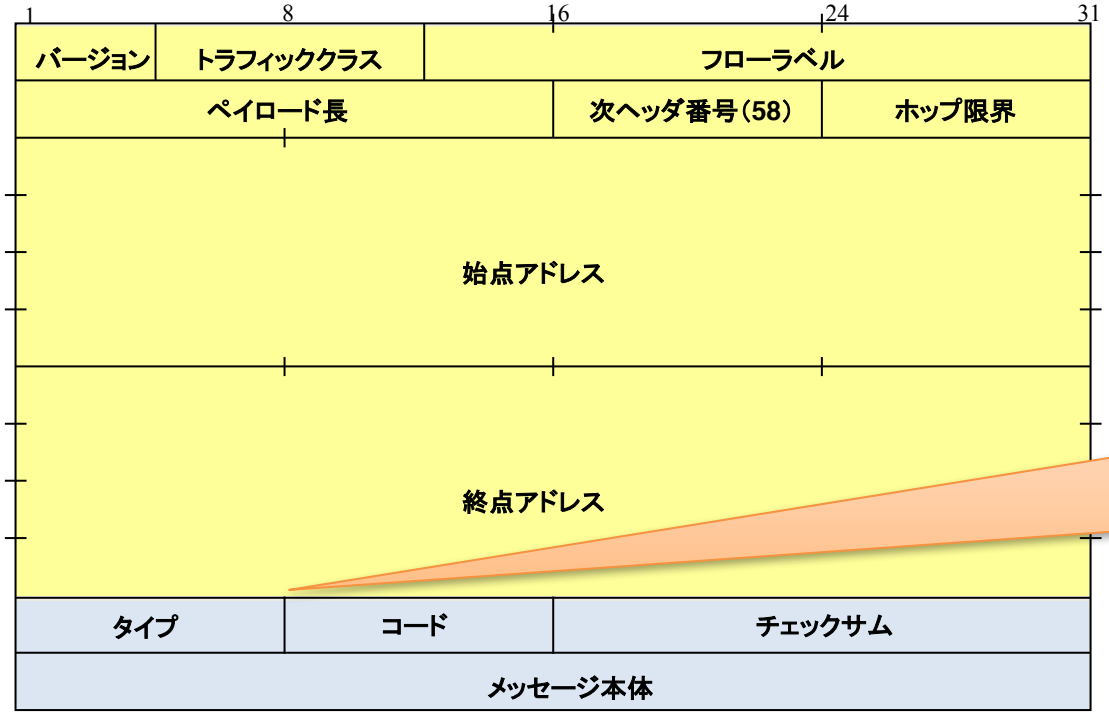


パスMTU探索

- パスMTU探索がうまくいかないと，所謂”パスMTUブラックホール”が発生
  - ユーザは，通信ができたり，出来なかったりという状況になる
  - システム的にも，
    - 届かないメールがある．サーバは，ping に返答する．
    - サーバには，ssh等ではログインできる
    - ファイルがたくさんあるディレクトリで ls すると固まる

    等といった，原因がわかりにくい事象となる．

ICMPv6パケットの構成



IPv6ヘッダ

タイプは8bit
- 0～127はエラー通知
- 128～255はそれ以外

コードは8bitで，Typeごとに定義された値

ICMPv6ヘッダ

ファイアウォール等でのICMPv6フィルタ設定

- **ICMP Error Message（type 0～127）**
  - Destination Unreachable（type 1）
  - Packet Too Big（type 2）
  - Time Exceeded（type 3）
  - Parameter Problem（type 4）
- **ICMP Informational Message（type 128～255）**
  - Echo Request（type 128）
  - Echo Reply（type 129）
  - Router Solicitation（type 133）
  - Router Advertisement（type 134）
  - Neighbor Solicitation（type 135）
  - Neighbor Advertisement（type 136）
  - Redirect Message (type137)

パスMTU探索を動作させるには，Type 2 のICMPv6メッセージを通過させることが必要

- それ以外にも，以下のICMPv6は通過させるべき
  - Destination Unreachable(Type 1)
    - TCP等がタイムアウトするまで通信できないことがわからない
    - IPv4へのフォールバックが遅くなる
  - Time Exceeded（type 3）
    - TCP等がタイムアウトするまで通信できないことがわからない
    - Traceroute6 が利用不可
  - Parameter Problem（type 4）
    - 障害解析が困難になる（エラーの原因がわからない）
      - ネクストヘッダタイプ異常（Code1）とIPv6オプション異常（Code2） 等

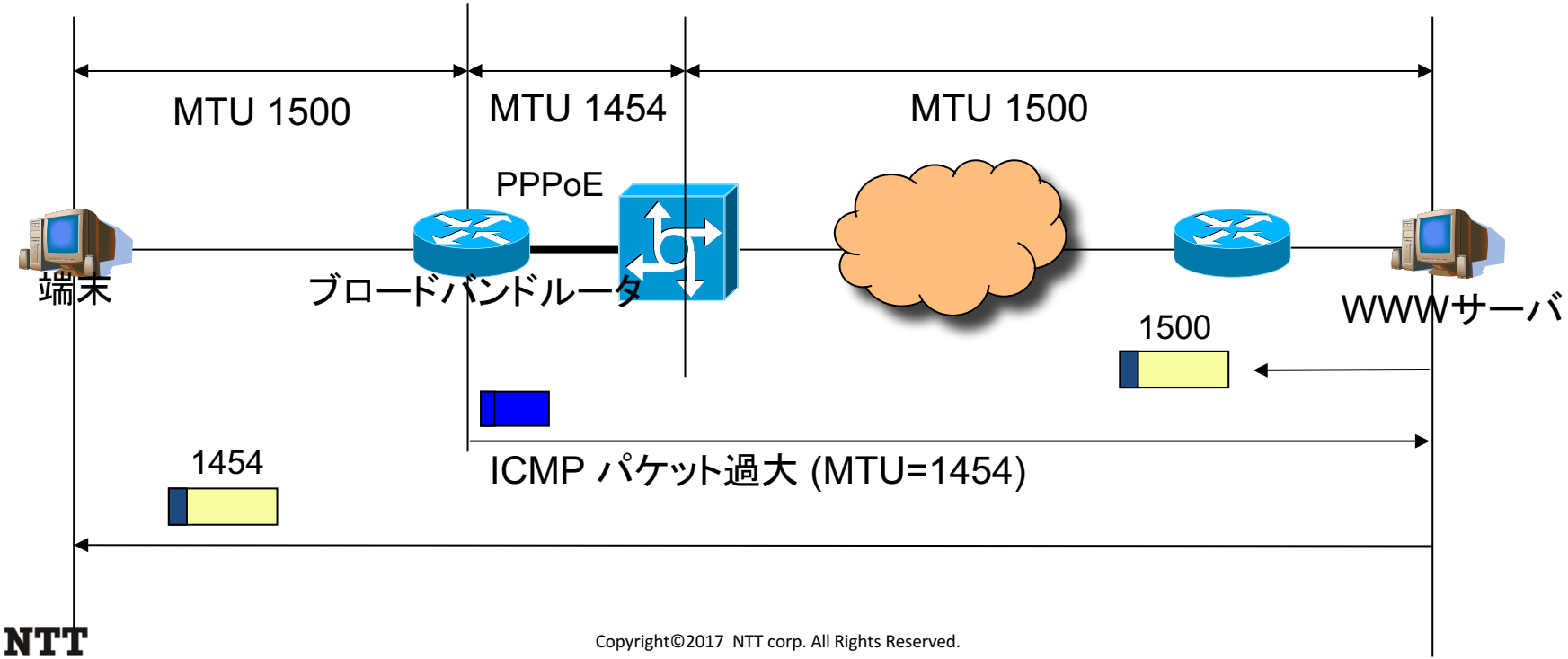
Innovative R&D by NTT

参考：ICMPとICMPv6の比較.

タイプ	ICMP	タイプ	ICMP6
0	Echo Reply	129	Echo Reply
3	Destination Unreachable	1	Destination Unreachable
4	Source Quench		
5	Redirect	137	Redirect
8	Echo Request	128	Echo Request
9	Router Advertisement	134	Router Advertisement
10	Router Solicitation	133	Router Solicitation
11	Time Exceed	3	Time Exceed
12	Parameter Problem	4	Parameter Problem
13	Timestamp		
		2	Packet too Big

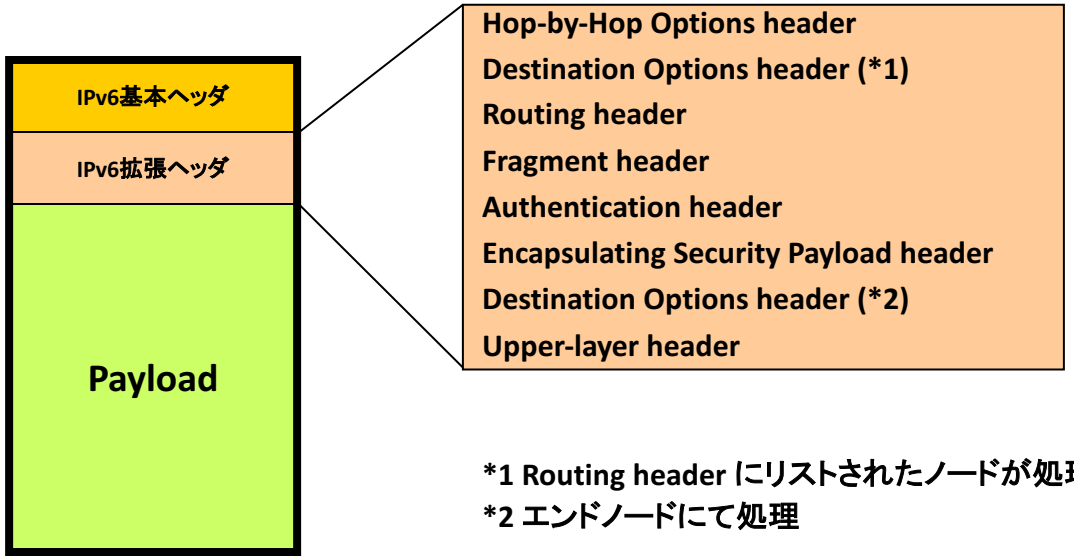
パスMTU探索問題：サーバの観点

- サーバもパスMTU探索を実施
  - サーバを設置する際に，入り口ルータのフィルタも同様に考える必要がある．



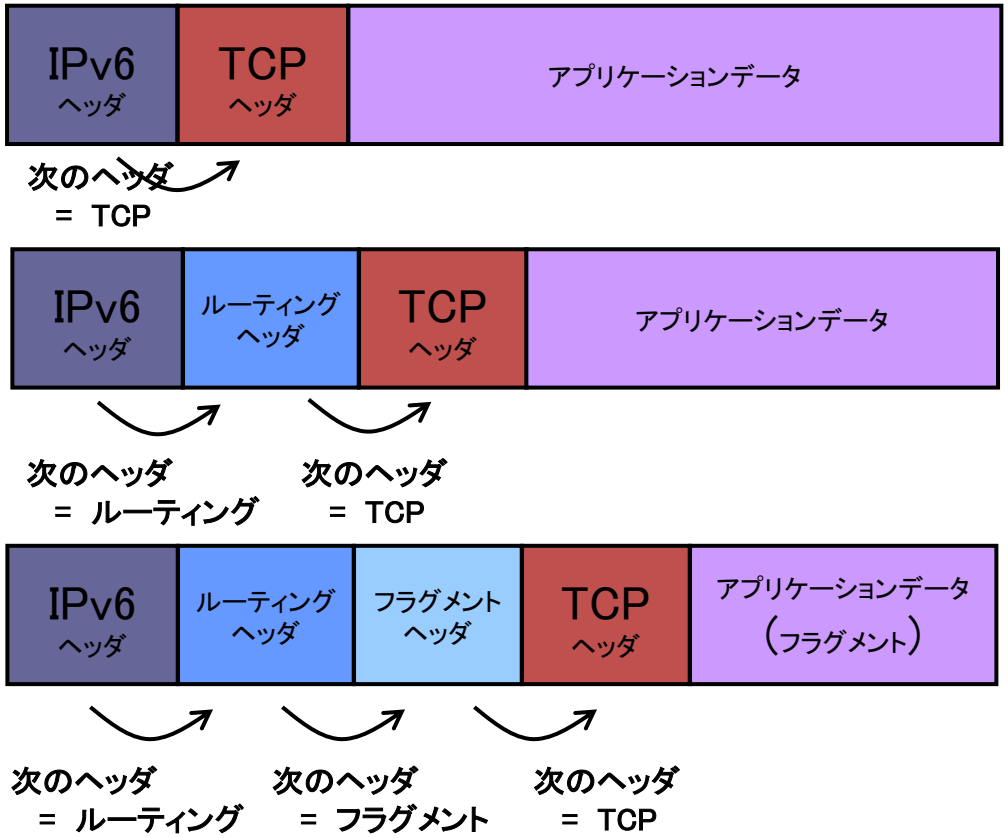
ファイアウォール設定：拡張ヘッダの扱い

- IPv6は，プロトコル自体の機能拡張をしやすいように，「拡張ヘッダ」が定義されている．
  - モバイルIPや，IPsecが拡張ヘッダを利用



*1 Routing header にリストされたノードが処理
*2 エンドノードにて処理

拡張ヘッダのチェーン



ファイアウォールでのフィルタの扱い

- IPv6にて，利用する機能に応じ，フィルタ設定を考慮する必要がある.
- 例：
  - IPsec を利用するためには，AH, ESPが必須
  - フラグメントパケットを扱うために，断片化ヘッダは通すべき（DNS等で必要）等

「拡張ヘッダ」入りパケットの扱いの現状

- 拡張ヘッダが付与されたパケットは，インターネット上でフィルタされる可能性あり.

Alexa's Top 1M Sites Dataset: Packet Drop Rate for Different Destination Types That Were Dropped in a Different AS

	Destination Option	Hop-by-hop option	Fragment
Web servers	10.91%	39.03%	28.26%
Mail servers	11.54%	45.45%	35.68%
Name servers	21.33%	54.12%	55.23%

RFC7872 より抜粋

経路途中での拡張ヘッダの取り扱い

- 経路途中で，拡張ヘッダをどう扱うべきかの議論が進んでいる．

  ”Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers”

  - https://tools.ietf.org/html/draft-ietf-opsec-ipv6-eh-filtering
- 拡張ヘッダごとに，推奨される扱い方，フィルタした場合の影響等を記述
- 例：IPsec EH (Protocol Number = 50)
  - Specific Security Implications
    - 宛先に対するDoS の手段として利用される可能性あり
  - Operational and Interoperability Impact if Blocked
    - IPsec の利用が出来なくなる
  - Advice
    - 中間システムでぇあ，EHパケットは通すべき

ドラフト段階！

LAN管理

LAN管理

- IPv6とIPv4の大きな違いの一つは，IPv6の近隣探索(ND: Neighbor Discovery)機構
  - NDに関するセキュリティ課題は多い
  - Insider による攻撃が多い，という報告があることからも重要

北口先生の「LAN管理」のお話に注意！

アドレス管理

アドレス管理

- アドレシング（どのようにアドレス設計をするか）は，セキュリティ向上に関する大きなポイント
  - リンクローカルアドレスによる通信
  - プライバシに関する課題
    - インタフェースID（IID）に利用する値
- ネットワークスキャン耐性
  - アドレス空間が広いため，スキャンは困難だと言われるが，割当方法や利用方法により，限定可能
  - IPv6のアドレシングアーキテクチャを理解し，場所・目的にあったアドレス利用や，アドレス割当方法を推奨

北口先生の「アドレス管理」のお話に注意！

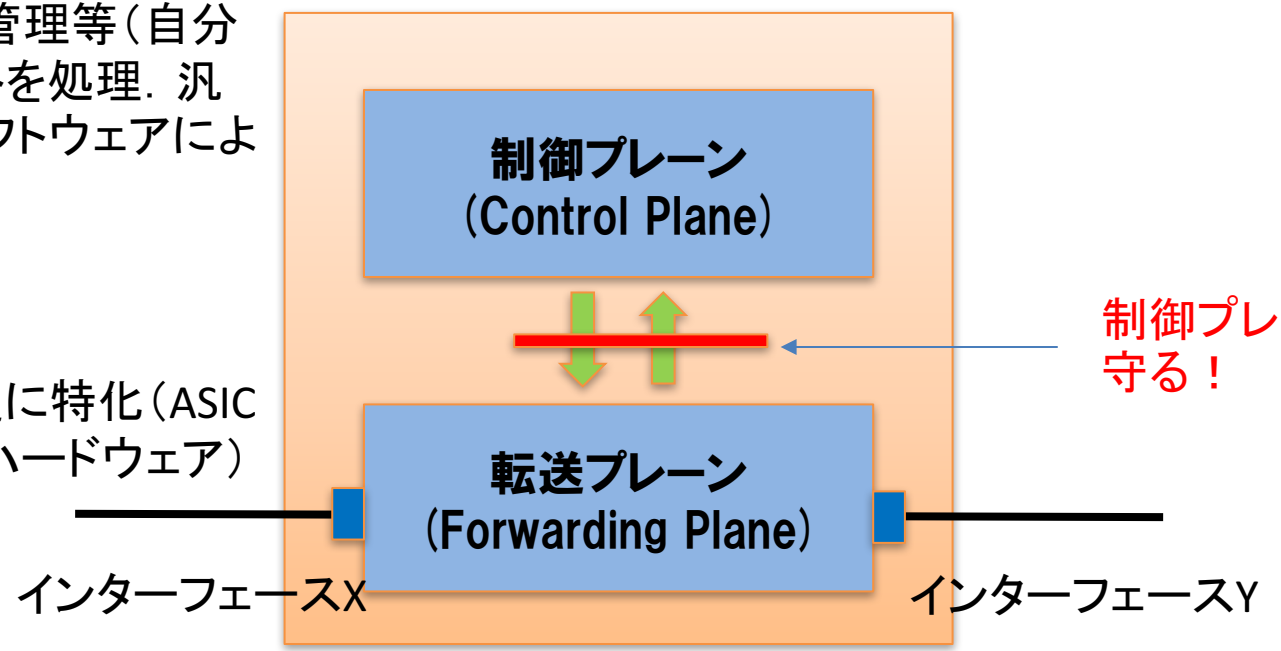
ルータ管理

昨今のルータアーキテークチャ

- DoS等にやられやすい，「制御プレーン」を守ることが重要．

経路計算，管理等（自分宛のパケットを処理．汎用のCPU,ソフトウェアによる構成）

パケット転送に特化（ASICによる専用ハードウェア）



制御プレーンの守り方

- 制御プレーンには，不正な制御パケットを渡さない
  - ACL 等で，フィルタする
- 制御プレーンのCPUの負荷を軽減するため，制御パケットのレートリミット等を実施
  - 不正なOSPFv6パケットにより余計な経路計算をさせるといった攻撃がある．経路計算の回数を制御することも必要．
- 対象となる制御パケットの種類
  1. 制御プロトコル：経路制御プロトコル（OSPFv3, BGP等），NDP, ICMP.
  2. 管理プロトコル：SSH, SNMP, IPfix, 等
  3. 例外パケット

制御プロトコル対策

対象：経路制御パケット（OSPFv3, BGP等）, NDP, ICMP

制御プレーン負荷軽減のため，全ルータインタフェースの入力フィルタに以下を設定することを推奨

- リンクローカルアドレス以外からの，OSPFv6パケット（次ヘッダ番号89），RIPngパケット（UDP ポート 521）を落とす
- BGPの接続先以外からのBGPパケット（TCPポート179）を落とす
- すべてのICMPパケットを許可（通過するもの，ルータのインタフェース宛のもの）

注：

- IPsec を利用した OSPFv3 を落とすことは不可能（ACLでは，IPsecの AH や ESP 拡張ヘッダを解釈できない）．
- 不正ないパケットも，レートリミットすべき．どの程度にするかは，制御プレーンのCPUの性能に依存

管理プロトコル対策

対象：SSH, SNMP, syslog, NTP 等

全ルータインタフェースの入力フィルタに以下を設定することを推奨

- 利用しているプロトコル外の，ルータ宛のパケットを落とす（例：SSHを利用している場合には，TCPのポート22を許可，他を落とす）
- セキュリティポリシに合致しない始点アドレスのパケットを落とす（例：NOCのアドレス以外からのSSHを落とす，等）

注：不正ないパケットも，レートリミットすべき．どの程度にするかは，制御プレーンのCPUの性能に依存

例外パケット対応

対象：制御プレーンでの処理を必要とする転送プレーン（データプレーン）のパケット

例：

- パケットが大きすぎて転送出来ず，ICMP パケット過大メッセージを生成する
- Hop-by-hop 拡張ヘッダの処理
- ルータの実装に依存する特定の処理（拡張ヘッダチェーンが長すぎてハードウェアで処理できない等）

- このようなパケットに対しては，レートリミット以外の手はない．

注：

- レートリミットをすると，パスMTU探索に必要な処理が落ち，パスMTUブラックホールを発生させる可能性がある．
- レートリミットは，入力側だけでなく，出力側（ICMP応答等）も必要（出力処理軽減，パケット増幅攻撃を防ぐ）．

経路制御のセキュリティ

「経路制御のセキュリティ」を担保するためには，一般的に，以下を考慮する必要がある

1. 近隣(Neighbor)/ピア を認証する
2. ピア間のルーティングアップデートを守る
3. 経路のフィルタを実施する

近隣/ピアの認証

- 経路制御の重要な要素：近隣ノード（ピア）との関係確立
- 近隣ノード（ピア）の認証
  - MD5や HMAC を利用し，経路制御を実施する前に相手を認証
  - OSPFv3：IPsec を利用可能だが，IPsec の実装はOSPFv3的には必須ではない
    - IPsec が使えないOSPFv3実装の場合には別途手当が必要
    - 歴史的経緯による実装の差に注意（AHの扱い等）
    - ESPを使うことで，経路情報自体も暗号化可能

ピア間のルーティングアップデートの保護

- OSPFv3 では，IPsec が利用できる．
- IPv6では，IPsec が利用可能？
  - 実際には，設定の難しさや，ハードウェア・ソフトウェアの制限から利用は困難な場合が多い．

経路のフィルタ

- 経路フィルタポリシは，目的や設定場所（外部からの経路をフィルタしたいのか，内部の経路なのか）によって違うが，基本的にIPv4と考え方は同等．

  例：
  - 内部経路や，グローバルに経路制御可能なIPv6アドレス以外をエッジで落とす．
  - 不正な経路，IANA等での予約経路は受け取らない・出さない
  - JPIRR, RADB等を参照し，正しい経路オリジン，プレフィックス所有者以外の経路を落とす，等
- IPv6での推奨フィルタ：
  - ”IPv6 Router Setting Reference”
  - http://www.team-cymru.org/templates/all-templates.html#ipv6-router-reference

ネットワークタイプ別セキュリティ考察
(IETFでの議論より)

ネットワークタイプ別セキュリティの考え方

以下の3種のネットワークにおけるIPv6セキュリティの考え方概略を解説

1. 企業ネットワーク
2. サービスプロバイダネットワーク
3. 家庭ネットワーク

企業ネットワークにおけるセキュリティ考察

- 外部との接続点におけるセキュリティ
  - ファイアウォールにおけるフィルタポリシは，IPv4のポリシから導出可能
  - 以下，更に注意すべき点：
    - 内部で利用しているIPv6アドレスを外部に出さない
    - 不正な IPv6アドレス，予約されていないIPv6アドレスからのパケットを内部に入れない
    - ICMPv6メッセージを適切に処理（PMTUD，ND等）
    - 拡張ヘッダを適切に処理（ESP, AH を通す，等）
      - 注：「次ヘッダ番号」でのフィルタの際，上位プロトコルをフィルタしないよう注意（TCP, UDP等）
    - 不正なIPv6ヘッダチェーンをもつパケットをフィルタ（双方）
    - 必要の無いサービスをフィルタ
    - Anti-spoofing 機構，レートリミット，制御プレーン制御機構を導入

企業ネットワークにおけるセキュリティ考察

- 内部におけるセキュリティ
  - IPv4と同じポリシを適用可能
  - 以下，IPv4との差分：
    - 近隣探索（ND: Neighbor Discovery) の扱い
    - IPv6 in IPv4 トンネルの扱い
    - ホストのファイアウォール（パーソナルファイアウォール）の実装
      - IPv4とIPv6を別に扱っておりポリシが違う，IPv6サポートなし，など
  - 注：
    - ホストでは，認証等のトランスポートにIPv4を使っていることが多い（RADIUS, TACACS+, SYSLOG など）．IPv6に関連する情報もこれら経由で通知されることがある．

- BGP
  - BGPにおけるセキュリティ考慮ポイントは，IPv4と同等.
    - TCPセッションの認証
    - TTLセキュリティ（IPv6ではホップ限界）
    - プレフィックスフィルタ
  - RTBH (Remote Triggered Black Hole Filtering)のIPv6用アドレスも定義されている.
    - 100::/64 (RFC6666)

家庭ネットワークにおけるセキュリティ概論

- 一般的に，家庭ネットワークは管理者不在
  - IPv6は既に多くのデバイス（PC, スマートフォン，アプライアンス等）で有効になっている
  - IPv6接続性がなくても，Terodo等のIPv4トンネルで接続する可能性あり
  - 家庭内は，リンクローカルアドレスで通信可能

パーソナルファイアウォール等での，IPv6対応（IPv4トンネル対応等も含む）が進展することが期待される．

- IPv6インターネットへの接続性があり，家庭用ゲートウェイ（RG: Residential Gateway）がある場合
  - RGでセキュリティの設定が可能
    - 現状，よく利用されているポリシ：
      - 外向け通信のみ許可：IPv4の NAT と同等．IPv6の利点である end-to-end 通信が出来ない
    - In/Out フルオープン，防御は各ノードで，という考え方もある．
    - Swisscom などでは，フルオープン＋α を利用しているとのこと
      - 基本，In/Out オープン，TCP/UDP の well-known ポートや，悪用されるポートを閉じる

今後のインターネット利用方法によって，変わってくると考えられる．

おわりに

- 「運用」観点からの，IPv6のセキュリティについて概観
- 今後のインターネットは，

  - IPv6/IPv4混在環境となる
  - QUICなどの新たなトランスポートプロトコルが利用される
  - IoTなど，新たな利用方法が広がる

  ため，TPOに合わせたセキュリティ対応が重要となる.