

実践！ IPv6ネットワーク構築 ～基礎概念編～

株式会社 インテック・ネットコア
北口善明

1) IPv6入門 IPv6の基礎知識のおさらい

**2) IPv6ネットワーク構築
小規模環境（家庭など）を想定した実技編**

内容：IPv6の基礎をおさらい

- 1-1. IPv6誕生の背景
- 1-2. IPv6の特徴
- 1-3. IPv6ヘッダ
- 1-4. IPv6アドレス表記法
- 1-5. IPv6アドレスの種類
- 1-6. プラグアンドプレイ
- 1-7. その他の機能
- 1-8. DNSの拡張
- 1-9. 移行技術

IPv4アドレスの枯渇問題

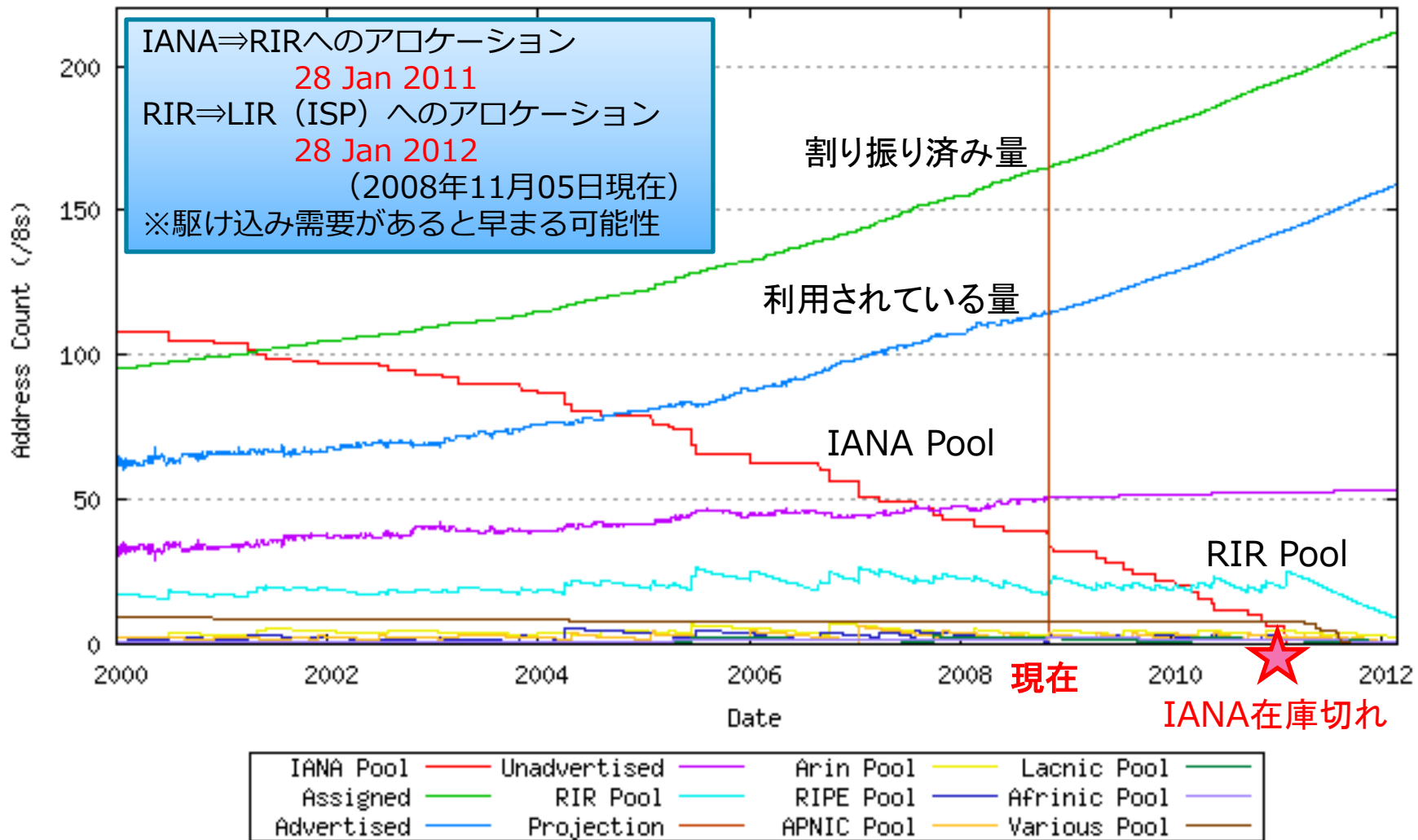
IPv4アドレスは32ビット=約43億個のアドレス数
インターネットの指数的な成長によるアドレス数の消費が加速

2010年には使い切るとの予想



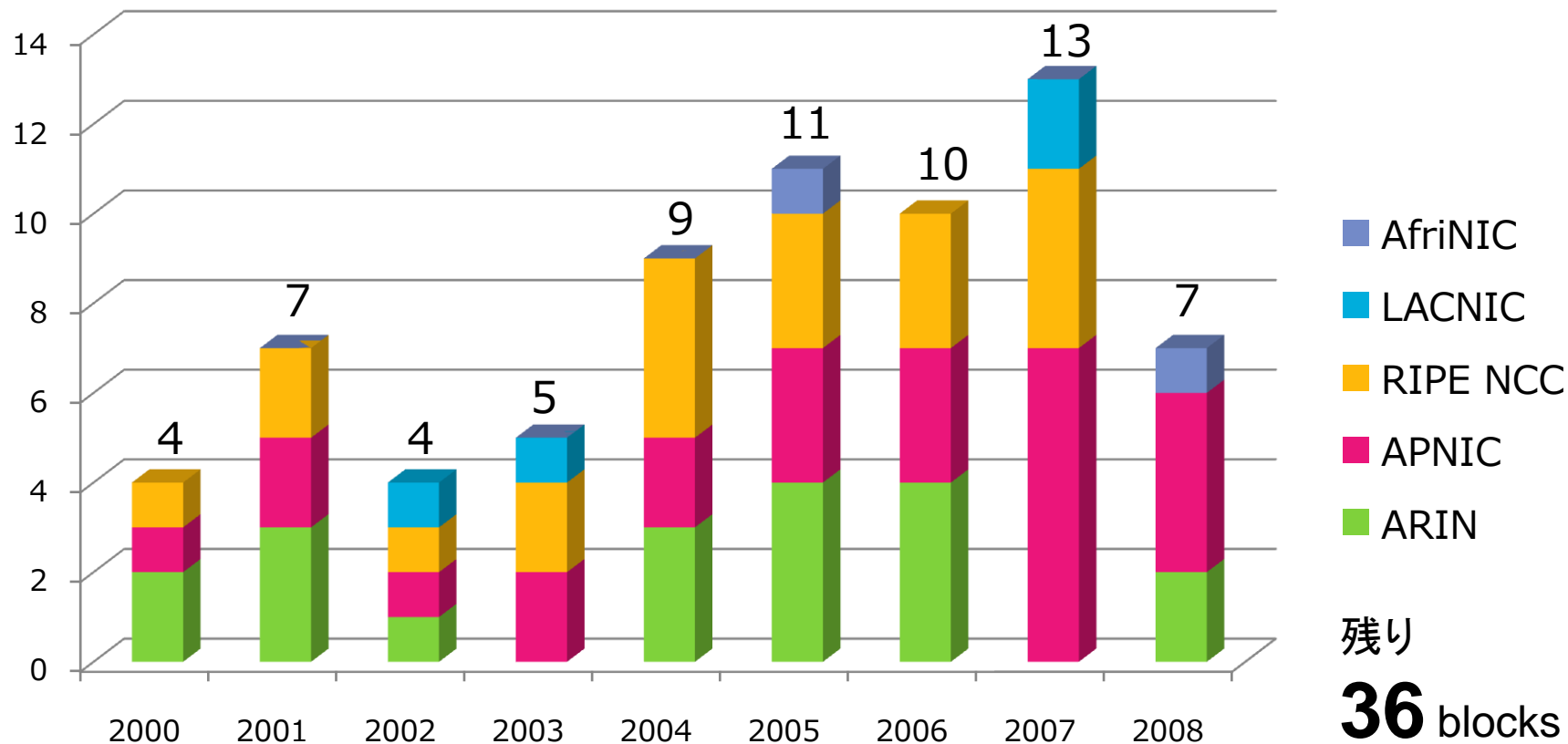
延命技術	メリット	デメリット
CIDR(Classless Inter-Domain Routing) クラス概念をなくしVLSMによる柔軟性のあるサブネットを構成可能にする技術	IPアドレスを効率的にセグメントに割り当てることが可能	特になし
プライベートアドレス ローカルネットワーク内で自由に利用可能なアドレス	ローカルで利用する端末でグローバルに一意的なアドレスを消費しない	特になし
NAT(Network Address Translation) プライベートアドレスとグローバルアドレスの変換を行う技術	ポート番号変換を併用(IPマスカレード/NAPT)することでグローバルアドレスを共有利用できる	IPアドレスをデータ部に含むアプリケーションが利用できない E2E通信ができない

1-1-1. IPv4アドレス枯渇予測



◆ Geoff Huston氏の最新予測より
<http://www.potaroo.net/tools/ipv4/>

/8アドレスブロックのRIRへの割り当て推移



※ 2008年11月現在

<http://www.iana.org/assignments/ipv4-address-space/>

広大なアドレス空間

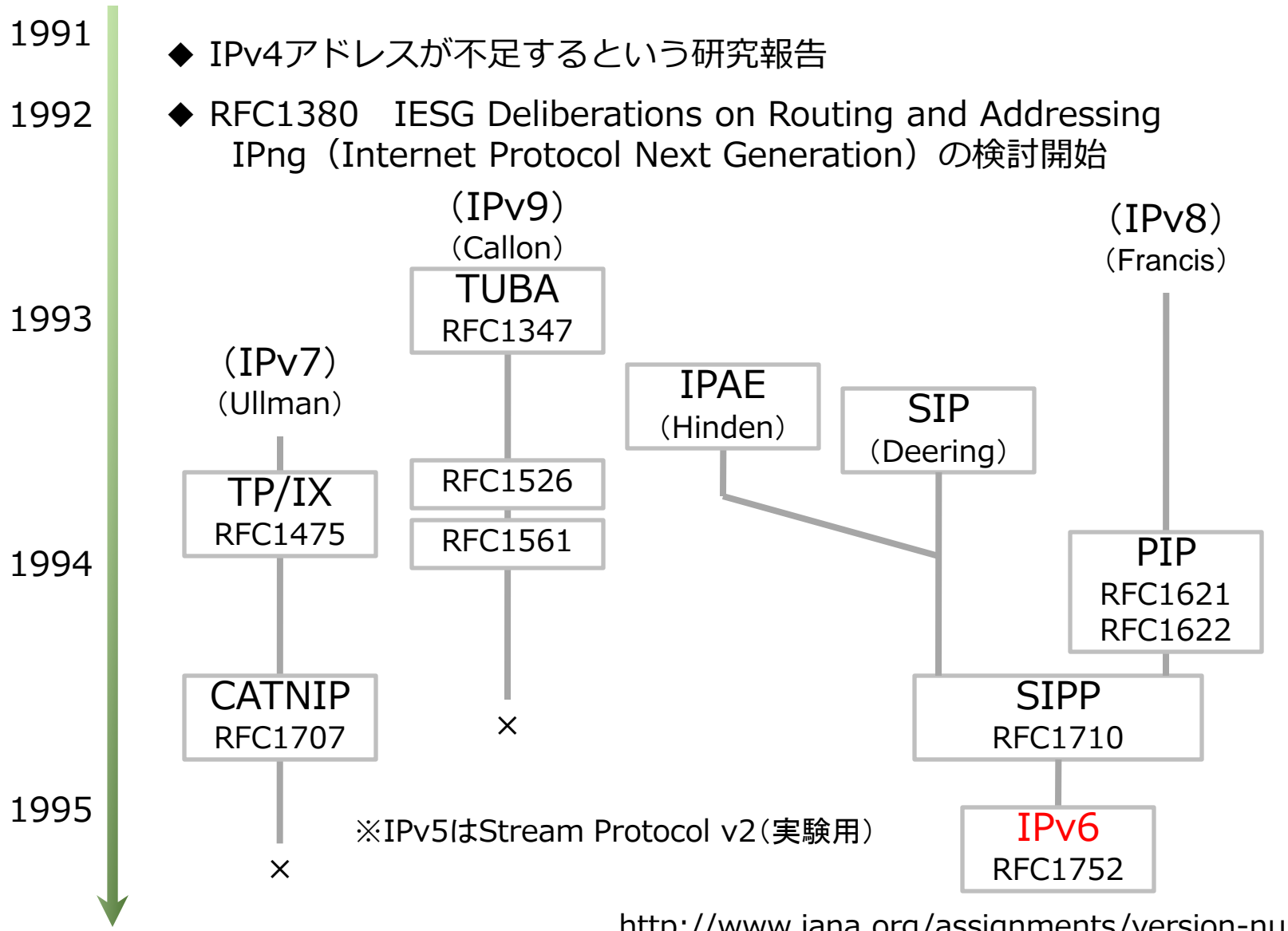
- 128ビットのアドレス
IPv4 : IPv6 = バケツの体積 : 太陽の体積
約340澗個 (澗 = 10^{36})
340,282,366,920,938,463,463,374,607,431,768,211,456個
- エンドツーエンド原理への回帰
本来のインターネットの姿 ⇒ NATによる通信障害がなくなる



追加された標準機能

- アドレス自動設定機能 (プラグアンドプレイ)
管理者やエンドユーザの利便性が向上
- セキュリティ機能 (IPsec) やマルチキャストの標準サポート
IPv4では追加機能だったものを標準装備
- QoSやモビリティの向上
QoS用のフィールドを準備 (ただし利用方法は未定)
拡張ヘッダを利用したモビリティ通信における経路最適化

1-2-1. IPv6誕生までの歴史



<http://www.iana.org/assignments/version-numbers>

◆簡易化されたヘッダ

- IPv4において利用されなかったフィールドの削除
代わりに新しい機能 (Flow Label) を追加
- 利用に即した名称に変更
Type of Service ⇒ Traffic Class
Total Length ⇒ Payload Length
Protocol ⇒ Next Header
Time to Live ⇒ Hop Limit

◆ルータへの負荷軽減

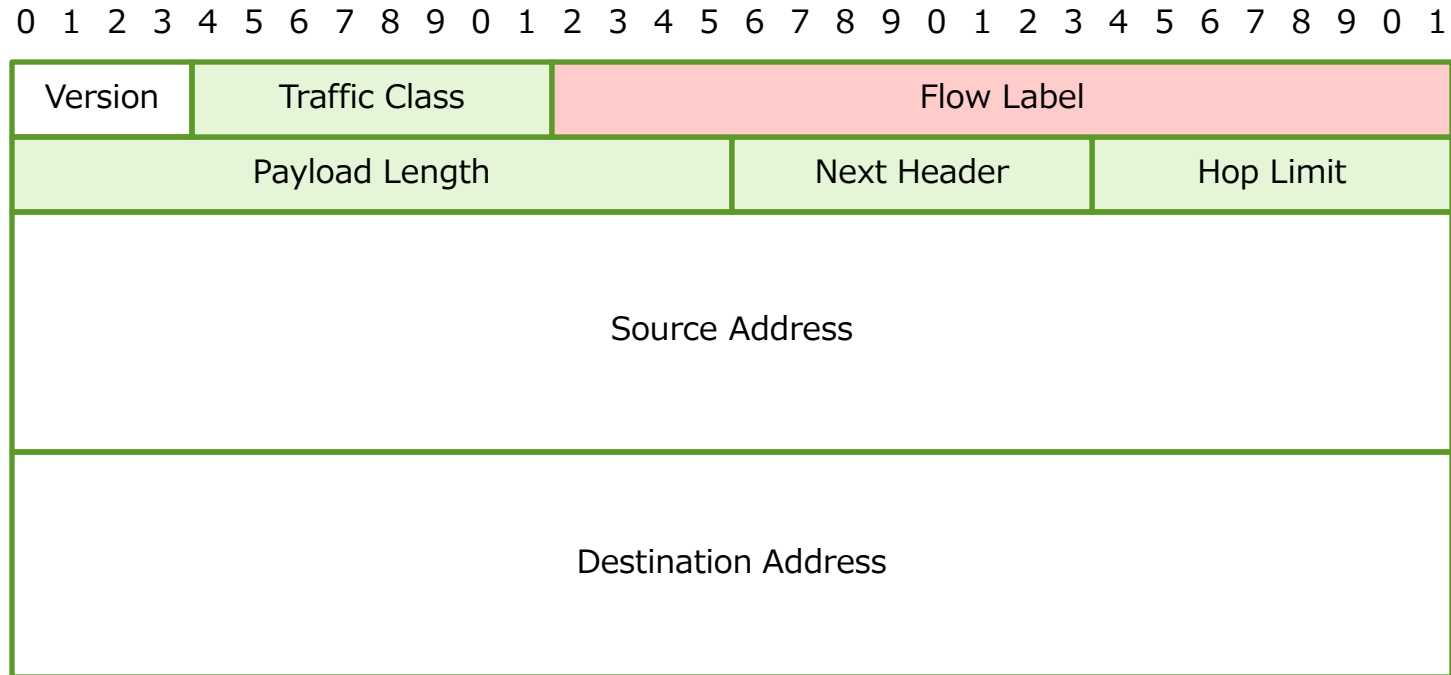
- フラグメント処理やオプションの分離
フラグメント処理はエンドノードでのみ実施とする
オプション機能は拡張ヘッダで実現しIPv6ヘッダは固定長とする



チェックサム機構の削除が可能
ルータではデータ長チェックが不要に

ルータにおけるパケット処理軽減を実現

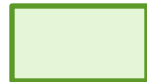
1-3-1. IPv6ヘッダフォーマット



※IPv6ではヘッダの長さは固定長

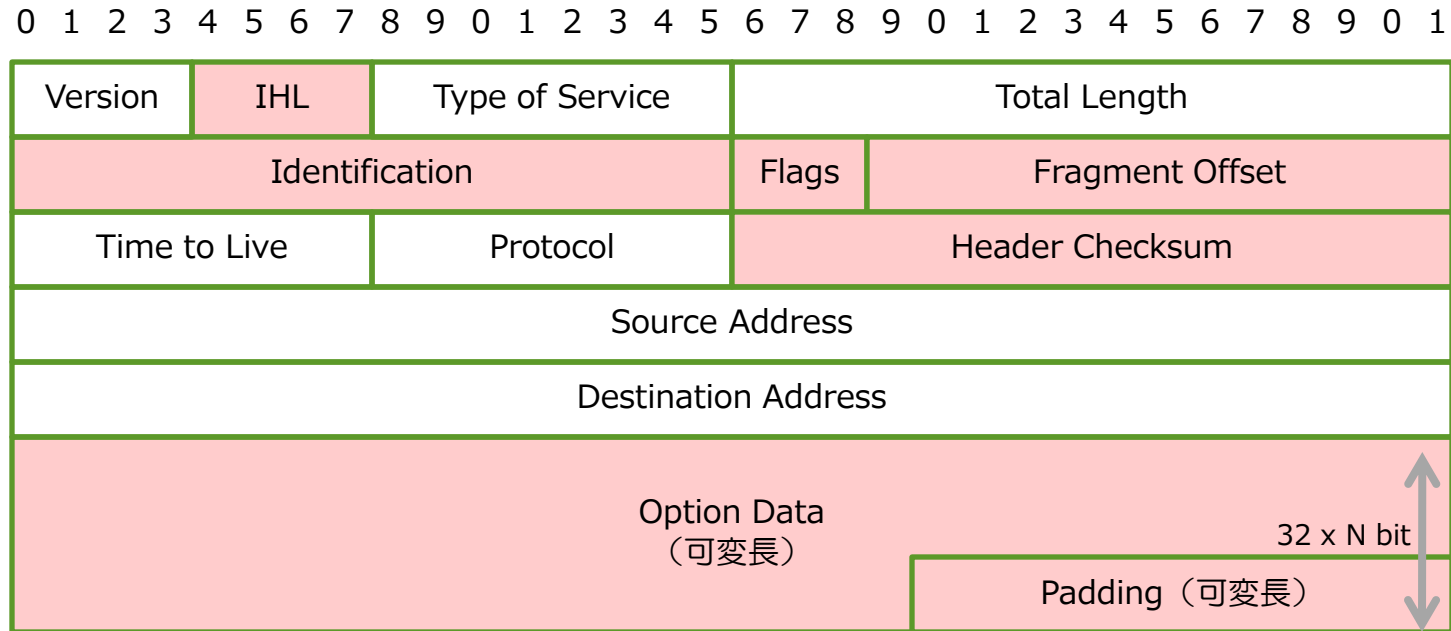



新設されたフィールド



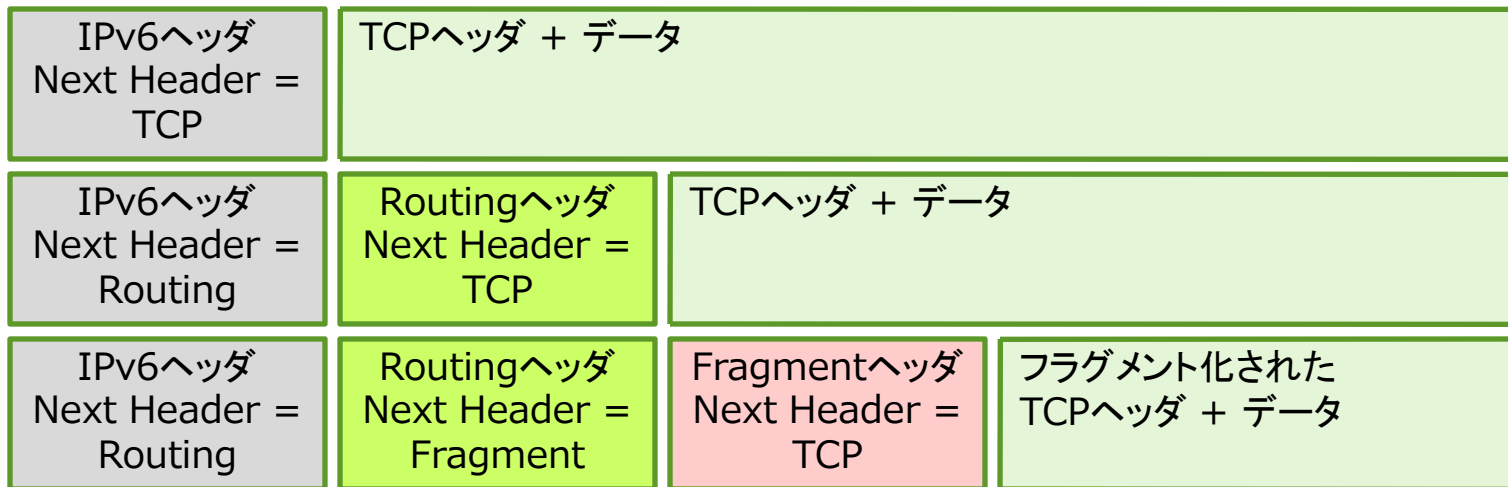
名称が変更されたフィールド（現状に則した名称に）

1-3-2. IPv4ヘッダフォーマット



 削除されたフィールド

◆ 拡張ヘッダによるヘッダの数珠つなぎ構造



◆ 定義済みの拡張ヘッダ

Protocol 番号	拡張ヘッダ名称	内容
0	ホップバイホップオプションヘッダ	中継ノードの処理を記述する
43	ルーティングヘッダ	送信元がルーティング経路を指定する <u>Type 0は利用禁止に (RFC5095)</u>
44	フラグメントヘッダ	パケット分割時に利用する 分割処理は送信ノードのみ
60	宛先オプションヘッダ	宛先ノードにて実行する内容を記述する
51	認証ヘッダ	エンドツーエンドにて完全性と認証を提供する
50	暗号ペイロード	IPsecにてペイロードを暗号化する際に利用する

◆IPv4のアドレス表記法

2進数表記 (32ビット)

```
11000000 10101000 00000000 00000001
```



・ 8ビットに区切り10進数で表現 区切り文字はピリオド「.」

```
192.168.0.1
```

◆IPv6のアドレス表記法

2進数表記 (128ビット)

```
0010000000000001 0000110110111000 1011111011101111 1100101011111110  
0000000000000000 0000000000000000 0000000000000000 0001001000110100
```



・ **16ビット**に区切り**16進数**で表現 区切り文字は**コロン**「:」

```
2001:0db8:beef:cafe:0000:0000:0000:1234
```



・ 省略表記① : 各ブロックの先頭の連続する「0」は省略可能

```
2001:db8:beef:cafe:0:0:0:1234
```



・ 省略表記② : 連続した「0」は1回に限り「::」に省略可能

```
2001:db8:beef:cafe::1234
```

◆IPv6アドレスの構造



- プレフィックス
グローバルルーティングプレフィックスとサブネットIDを合わせた
上位64ビット

◆IPv6アドレスの種類

- ユニキャストアドレス 1対1 通信
ネットワークインターフェイス毎に設定されるアドレス
グローバルアドレス, リンクローカルアドレス, ULA
- マルチキャストアドレス 1対多 通信
グループを識別するアドレスで複数のノードを識別
IPv6ではIPv4のブロードキャストの置き換えとして利用
- エニーキャストアドレス 1対1 of多 通信
複数のノードに指定可能な「機能」に対して設定されるアドレス

◆グローバルユニキャストアドレス



(3ビット)

48ビット

16ビット

64ビット

・いわゆるグローバルアドレス (例) 2001:db8::1

◆リンクローカルユニキャストアドレス



10ビット

54ビット

64ビット

・同一リンク (セグメント) 内にて一意なアドレス (fe80::/10)
プラグアンドプレイなどのリンク内通信で利用される

◆ユニークローカルユニキャストアドレス (ULA)

[RFC4193]



8ビット

16ビット

64ビット

Lビット: 0 登録制 (将来利用) 1 ランダム生成による独自割り当て

- ・自由に利用可能なローカルアドレス (fd00::/8)
- ・廃止されたサイトローカルアドレスの代用

◆未指定アドレス

- アドレスが未割り当てのときに送信元アドレスとして利用
すべて0のアドレス $0:0:0:0:0:0:0:0 = ::$

◆ループバックアドレス

- 自分自身を表すアドレス (IPv4における127.0.0.1)
最下位ビットのみ1 $0:0:0:0:0:0:0:1 = ::1$

◆共存技術用アドレス

- IPv4射影アドレス (IPv4-mapped IPv6 address) $:::ffff:0:0/96$
IPv6アプリケーション側からIPv4アドレス扱うためのアドレス
表記方法 $0:0:0:0:0:ffff:<w.x.y.z>$ 例) $ffff:192.168.0.1$
- IPv4互換アドレス (IPv4-compatible IPv6 address) $:::/96$
IPv4ネットワークを利用した自動トンネル接続に利用するアドレス
表記方法 $0:0:0:0:0:0:<w.x.y.z>$ 例) $:::192.168.0.1$
⇒RFC4291において利用が非推奨に
- その他の自動トンネルアドレス
6to4アドレス, Teredoアドレス, ISATAPアドレス

◆マルチキャストアドレスの構造

11111111	フラグ ORPT	スコープ	グループID
8ビット	4ビット	4ビット	112ビット

フラグ	意味
Tフラグ	0 : 恒久的な割り当て (IANAにより定義済み) アドレス 1 : 一時的な割り当てアドレス
Pフラグ	1 : Unicast-Prefix-basedマルチキャストアドレス (RFC3306) ※P=1の場合にはT=1
Rフラグ	1 : PIM-SMにおけるRendezvous Point (RP)マッピング用 (RFC3956) ※R=1の場合P=1 T=1

スコープ : マルチキャストの有効範囲を指定

0000 (0)	予約	0101 (5)	site-local scope
0001 (1)	interface-local scope	1000 (8)	organizational-local scope
0010 (2)	link-local scope	1110 (E)	global scope
0100 (4)	admin-local scope	1111 (F)	予約

◆定義済みのマルチキャストアドレス

FF02:0:0:0:0:0:0:1	リンク内のすべてのIPv6ノード (IPv4のブロードキャストの代用)
FF02:0:0:0:0:0:0:2	リンク内のすべてのIPv6ルータ
FF02:0:0:0:0:0:0:C	DHCPサーバ/リレーエージェント
FF02:0:0:0:0:1:FFxx:xxxx	要請ノードマルチキャストアドレス (xxxxxxはMACアドレスの下24ビット)

◆エニーキャストアドレス

- 複数の機器に付与され最も近いものに転送（負荷分散などで利用）
- 見た目はユニキャストアドレスと同じ
- IPv6で登場した概念（IPv4にも導入された：ルートDNSなど）

◆サブネットルータエニーキャストアドレス

サイトプレフィックス	インターフェイスID 全て0 (0000 0000 0000 0000)
64ビット	64ビット

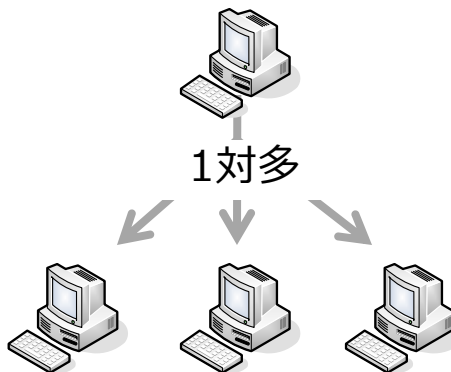
- 特定のプレフィックスを持つサブネット上のルータを表す

◆通信形態の比較

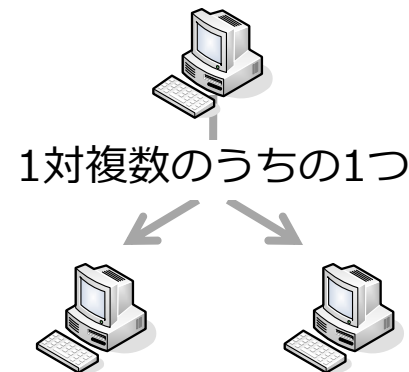
ユニキャスト



マルチキャスト



エニーキャスト



◆ステートレス自動アドレス設定

- エンドノードに自動的にアドレスを付与する技術
ルータ以外に特別なサーバを必要としないが細かな制御は困難

◆インターフェイスIDの自動生成

①MACアドレスからの生成 (EUI-64形式)

MAC address : 00:A0:F8:01:6A:B8
⇒ インターフェイスID : 2a0:f8ff:fe01:6ab8

②プライバシー拡張アドレス (RFC4941)

インターフェイスIDにランダムな値を用いる一時アドレスを利用
一定時間 (最大7日間) で更新しノードの特定を困難にする

◆IPv6アドレスとデフォルト経路の設定 (近隣探索プロトコル)

- ルータ広告 (RA) によるデフォルト経路とプレフィックスの設定
デフォルト経路 : ルータ広告発信元のリンクローカルアドレス
プレフィックス : (例) 2001:db8:cafe:1::/64
- アドレス重複検出 (DAD) によるアドレス決定
リンク内におけるアドレス重複を調査して利用アドレスを決定
リンクローカルアドレス : fe80::2a0:f8ff:fe01:6ab8
グローバルアドレス : 2001:db8:cafe:1:2a0:f8ff:fe01:6ab8

◆近隣探索プロトコル（NDP）の主な機能

- セグメント内で一意なIPアドレスを決定する仕組みを実現
- デフォルト経路やネットワークプレフィックスの配布
- リンクレイヤアドレスの解決（IPv4におけるARP）

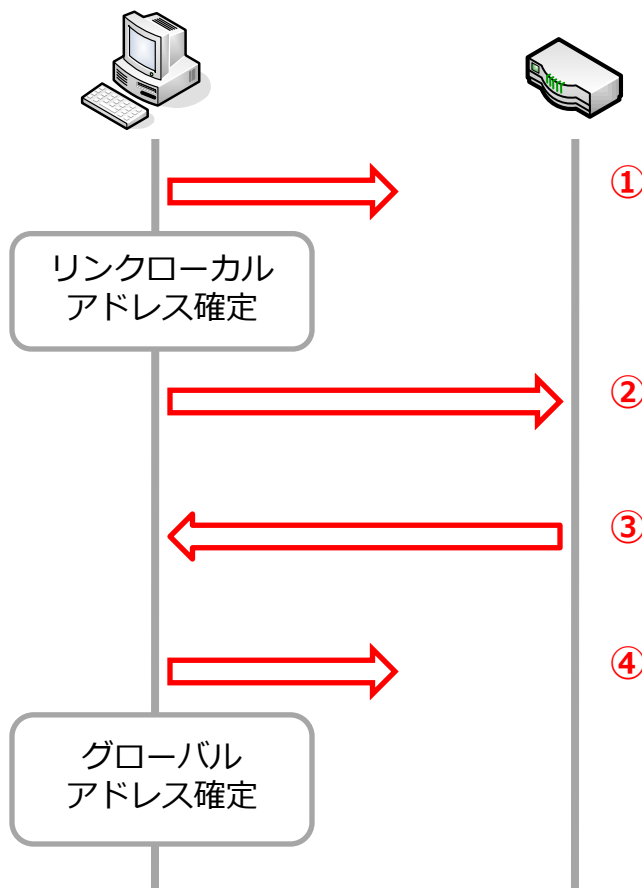
◆5つのメッセージタイプ（ICMPv6機能の一部）

メッセージ	役割
近隣要請 NS : Neighbor Solicitation	重複アドレス検出（DAD）や到達性／不到達性の確認，リンクレイヤアドレスの解決（IPv4のARPと同様）
近隣広告 NA : Neighbor Advertisement	近隣要請に対する応答 自身のアドレス変更通知では単独利用となる
ルータ要請 RS : Router Solicitation	セグメント内のルータ発見に利用 ルータ広告を即座に取得する場合に送出
ルータ広告 RA : Router Advertisement	ルータによるデフォルト経路の通知 プレフィックス情報配布で自動アドレス設定が可能になる
リダイレクト	IPv4におけるリダイレクトと同様

1-6-2. ステートレス自動アドレス設定手順

MAC:00:11:22:33:44:55

MAC:00:11:22:66:77:88



- ①近隣要請 (NS)
 近隣広告がなければ
 ターゲットアドレス
 の利用が可能
 <重複アドレス検出>

要請ノードマルチキャスト

- ②ルータ要請 (RS)
 全ルータマルチキャスト
 (ff02::2) 宛に送信

- ③ルータ広告 (RA)
 全ノードマルチキャスト
 (ff02::1) 宛に送信
 取得プレフィックス
 を用いてグローバル
 アドレスを生成

- ④近隣要請
 近隣広告がなければ
 ターゲットアドレス
 の利用が可能
 応答があるとアドレス
 を再構成する必要あり
 <重複アドレス検出>

Src MAC	00:11:22:33:44:55
Dst MAC	33:33:FF:33:44:55
Src IPv6	:: (未定義アドレス)
Dst IPv6	ff02::1:ff33:4455
ICMPv6 Type	135
Target	fe80::211:22ff:fe33:4455

Src MAC	00:11:22:33:44:55
Dst MAC	33:33:00:00:00:02
Src IPv6	fe80::211:22ff:fe33:4455
Dst IPv6	ff02::2
ICMPv6 Type	133

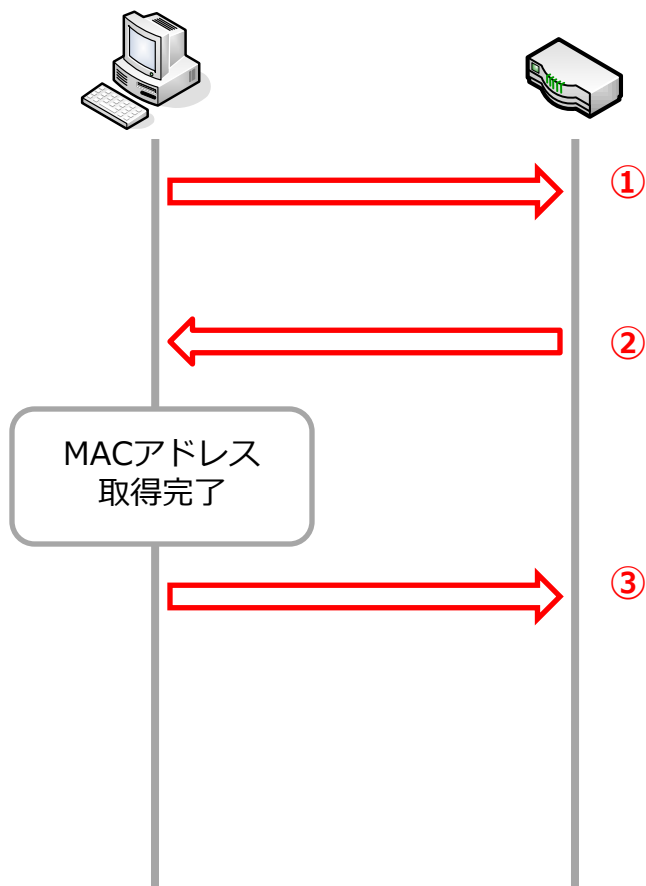
Src MAC	00:11:22:66:77:88
Dst MAC	33:33:00:00:00:01
Src IPv6	fe80::211:22ff:fe66:7788
Dst IPv6	ff02::1
ICMPv6 Type	134
Prefix	2001:db8::

Src MAC	00:11:22:33:44:55
Dst MAC	33:33:FF:33:44:55
Src IPv6	:: (未定義アドレス)
Dst IPv6	ff02::1:ff33:4455
ICMPv6 Type	135
Target	2001:db8::211:22ff:fe33:4455

1-6-3. リンクレイヤアドレスの解決手順

MAC:00:11:22:33:44:55

MAC:00:11:22:66:77:88



- ①近隣要請 (NS)
通信相手のMACアドレスを探索
近隣広告がない場合は
オンリンクでないと判断

Src MAC	00:11:22:33:44:55
Dst MAC	33:33:FF:66:77:88
Src IPv6	fe80::211:22ff:fe33:4455
Dst IPv6	ff02::1:ff66:7788
ICMPv6 Type	135
Target	2001:db8::211:22ff:fe66:7788

- ②近隣広告 (NA)
ターゲットアドレスを
持つノードが回答
ただし誰でもこの応答は
可能

Src MAC	00:11:22:66:77:88
Dst MAC	00:11:22:33:44:55
Src IPv6	fe80::211:22ff:fe66:7788
Dst IPv6	fe80::211:22ff:fe33:4455
ICMPv6 Type	136
Target	2001:db8::211:22ff:fe66:7788
Target MAC	00:11:22:66:77:88

- ③通信開始

1-6-4. ルータ広告のメッセージフォーマット

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type = 134				Code = 0				Checksum													
Cur Hop Limit				M	O	H	Prf	P	Res	Router Lifetime											
Reachable Time																					
Retrans Timer																					
Options																					

フィールド名	意味
Type	ICMPv6のタイプ ルータ広告は134
Cur Hop Limit	IPヘッダのホップ限界フィールドに設定するデフォルト値を指定
M Flag	1：ステートフルアドレス自動設定をノードに促す（ステートフルDHCPv6利用）
O Flag	1：他の設定情報取得をノードに促す（ステートレスDHCPv6利用）
H Flag (RFC3775)	1：このルータ広告を送っているルータがMIPv6におけるホームエージェントであることを示す
Prf Flag (RFC4191)	デフォルトルートになりえるルータの優先度を指定 00：Medium 01：High 11：Low
Router Lifetime	ルータの有効時間を秒で指定（0の場合はデフォルトルートとして扱えないことを意味）
Reachable Time	到達可能性確認を受け取ってから利用可能になるまでの時間をミリ秒で指定
Retrans Timer	近隣要請メッセージを送信する間隔をミリ秒で指定

◆ステートフル自動アドレス設定

- エンドノードに管理サーバによりアドレスを付与する技術
DHCPが一般的に利用される
ノードに割り当てたアドレスの管理が可能
- DHCPv6 (Dynamic Host Configuration Protocol Version 6)
DHCPサーバによりネットワークの構成情報を配布
DNSサーバ情報の通知やアドレス管理が可能
ルータ広告のMフラグやOフラグにより利用を促すことが可能
※ただし現時点でのRFCではフラグの利用は明確になっていない
- ルータ広告とDHCPv6の違い
ルータ広告はDNSサーバなどのネットワーク情報を設定できない
DHCPv6はデフォルト経路やプレフィックス情報を設定できない

◆プレフィックス委譲 (Prefix Delegation)

- プレフィックス単位での割り当てを実現する仕組み
DHCPv6の拡張機能 (DHCPv6-PD) により実現



◆IPv6のセキュリティ機能

- IPsecを考慮した設計
 - IPv4では後付け機能のIPsecを標準実装（拡張ヘッダの一部）
 - 認証ヘッダ（AH）：認証，完全性を提供
 - 暗号ペイロード（ESP）：認証，完全性，機密性を保証
- 鍵管理（IKE）
 - IPv6の範囲外で定義し柔軟な暗号化技術の利用が可能

◆IPv6のモビリティ機能

- モバイルIPv6（MIPv6）
 - 経路最適化のために用意された拡張ヘッダ
 - ルーティングヘッダ（Type 2）：経由ルータを1つだけ指定可能
 - 宛先オプションヘッダ（Home Address Option）：HoAを指定
- NEMO（Network Mobility）
 - IPv6におけるネットワークの移動性を提供する

◆IPv6のQoS機能

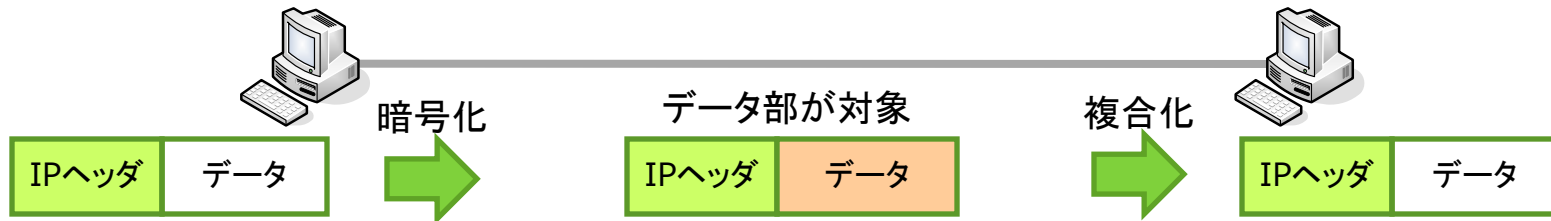
- IPv6で登場したフローラベル（Flow Label）
 - IPv6ヘッダに定義されているが利用方法は明確になっていない

◆IPsecの主な機能

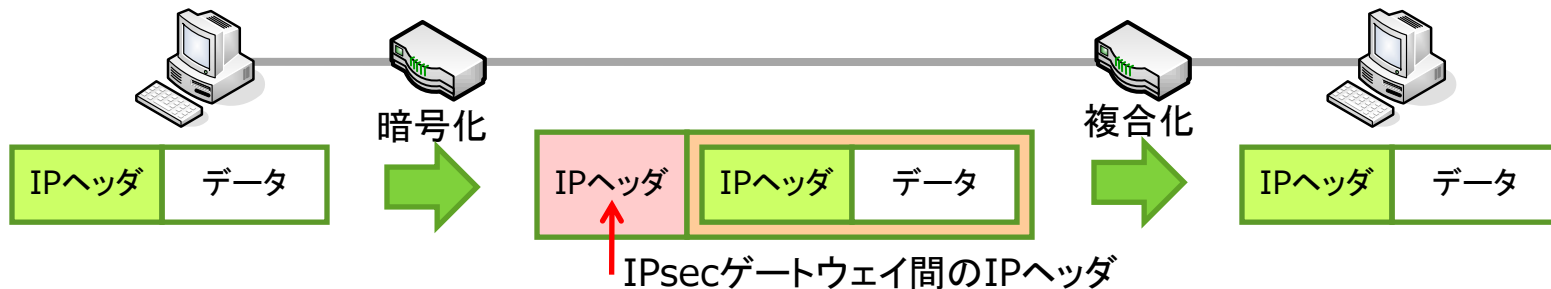
- インターネット層におけるセキュリティ技術
- IPパケットの暗号化と認証
- IPパケットの改竄防止

◆二つのモード

- トランスポートモード（端末間のセキュリティ）
データ部分のみが認証・暗号化の対象

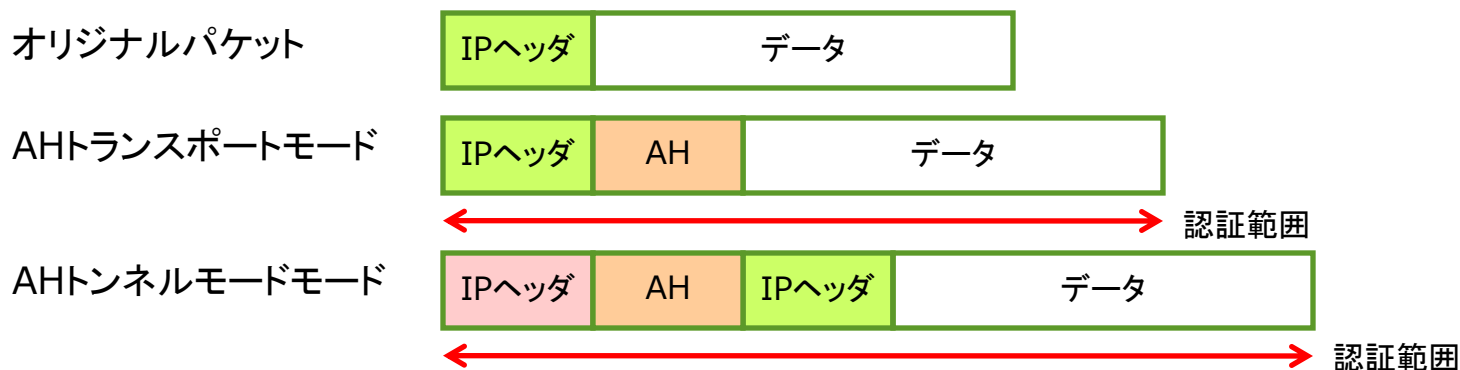


- トンネルモード（サイト間のセキュリティ）
IPパケット全体が認証・暗号化の対象



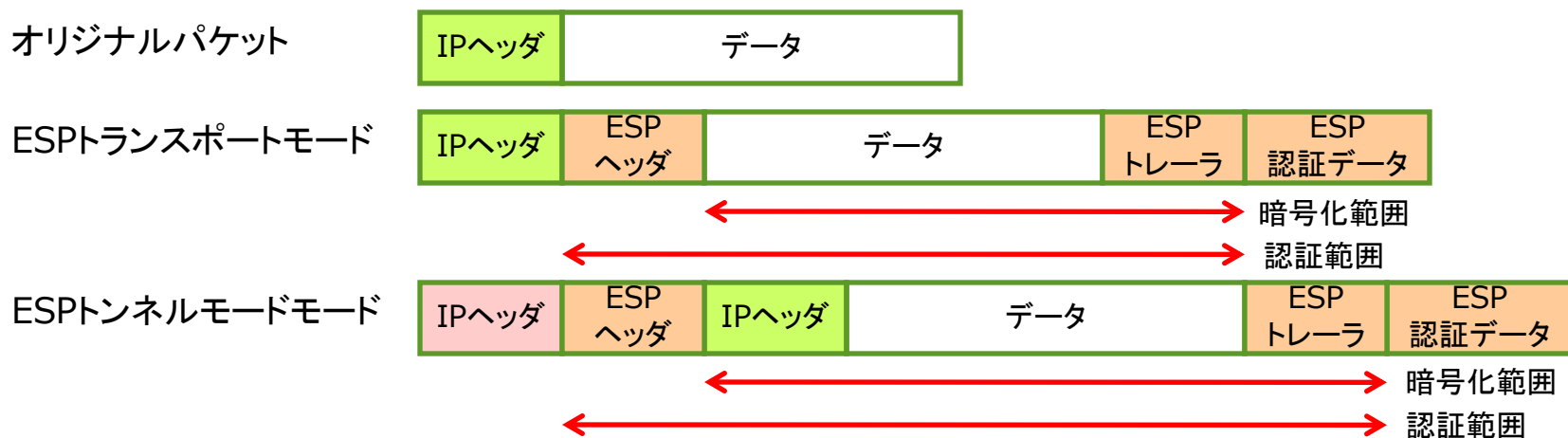
◆ 認証ヘッダ (AH)

- 認証と完全性を提供



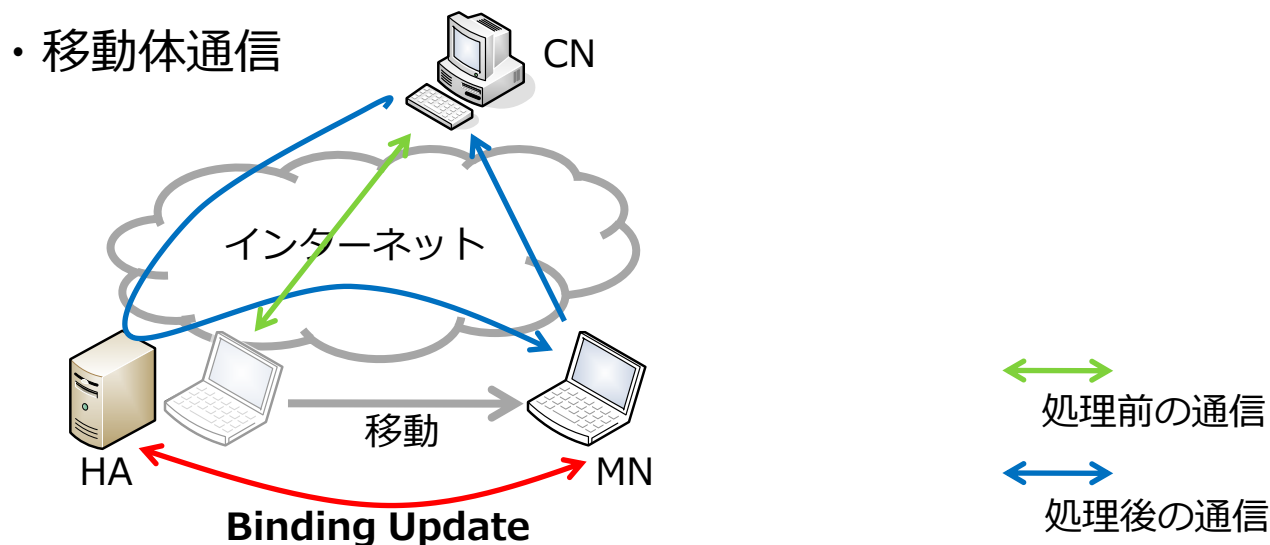
◆ 暗号ペイロード (ESP)

- 認証と完全性を提供し、機密性を保証



◆MIPv6の主な機能

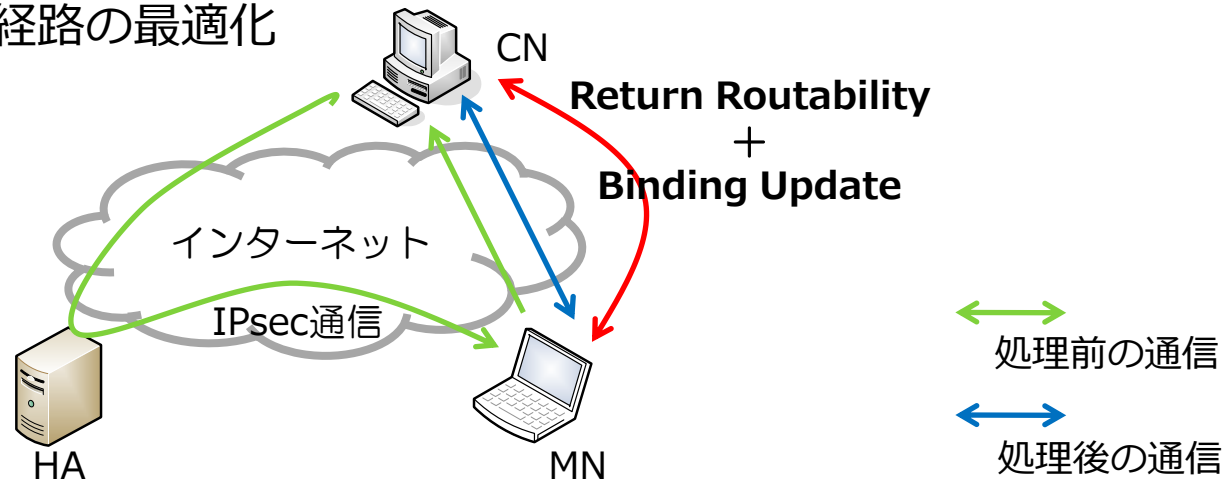
- IPレベルでの移動体通信を実現
同じIPアドレス（ホームアドレス：HoA）を利用する
ホームエージェント（HA）が通信を中継することで実現
- アドレス結合更新（Binding Update）
移動ノード（MN）の気付アドレス（CoA）を登録し転送処理
- 往復経路確認（Return Routability）
MNと通信相手（CN）間で認証情報を交換
HAを介さない直接通信を実現



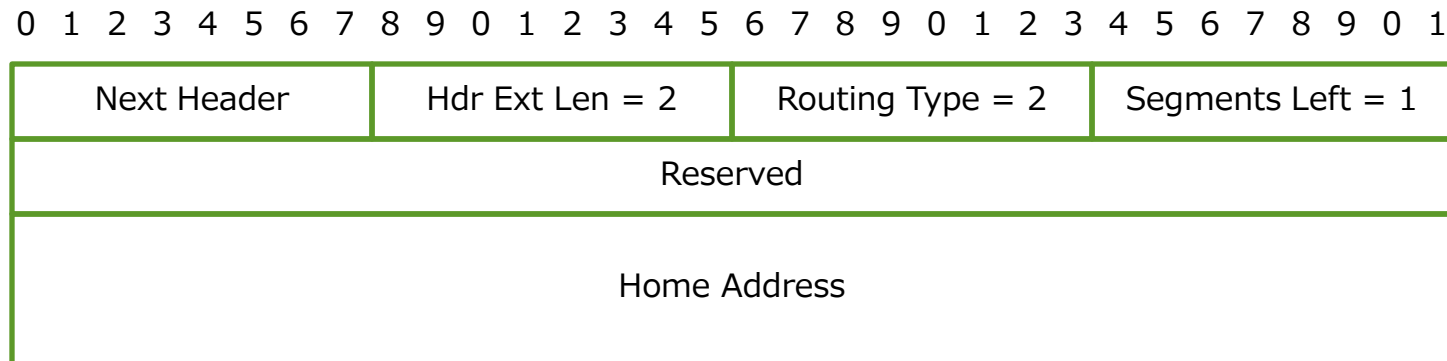
◆MIPv6の利点

- 三角通信問題の解消
MNの送信元アドレスにCoAを利用可能
ルーティングヘッダと宛先オプションヘッダの利用によりMNとCNの直接通信を実現可能
- アドレス自動設定機能の標準装備
移動先ネットワークでも容易にCoAを取得可能
- IPsecを利用したセキュリティの向上
IPv6ではIPsecが標準実装であるのでMIPv6では積極的に利用
HA-MN間の通信の暗号化などに利用

・ 経路の最適化

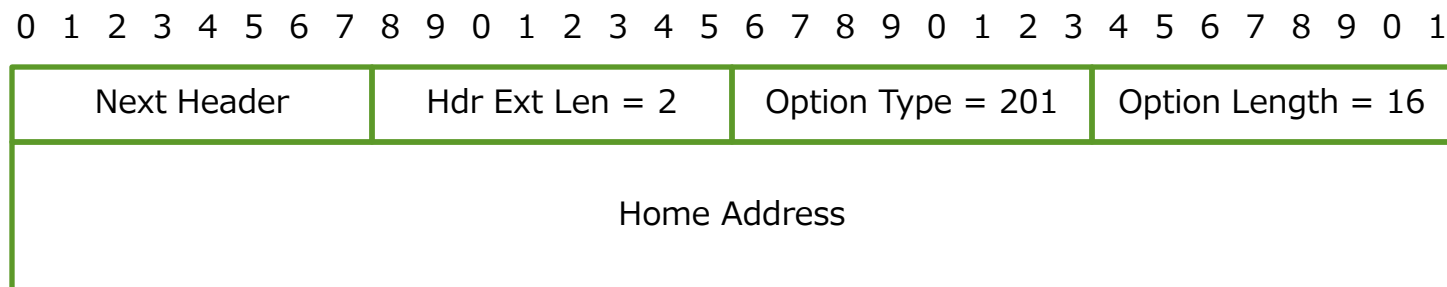


◆ルーティングヘッダ (Type 2)



※受信ノードは宛先アドレスとRoutingヘッダ内のHoAを入れ替えて転送
MIPv6ではMNがHoAも自身のアドレスとして持つので再び受信することになる

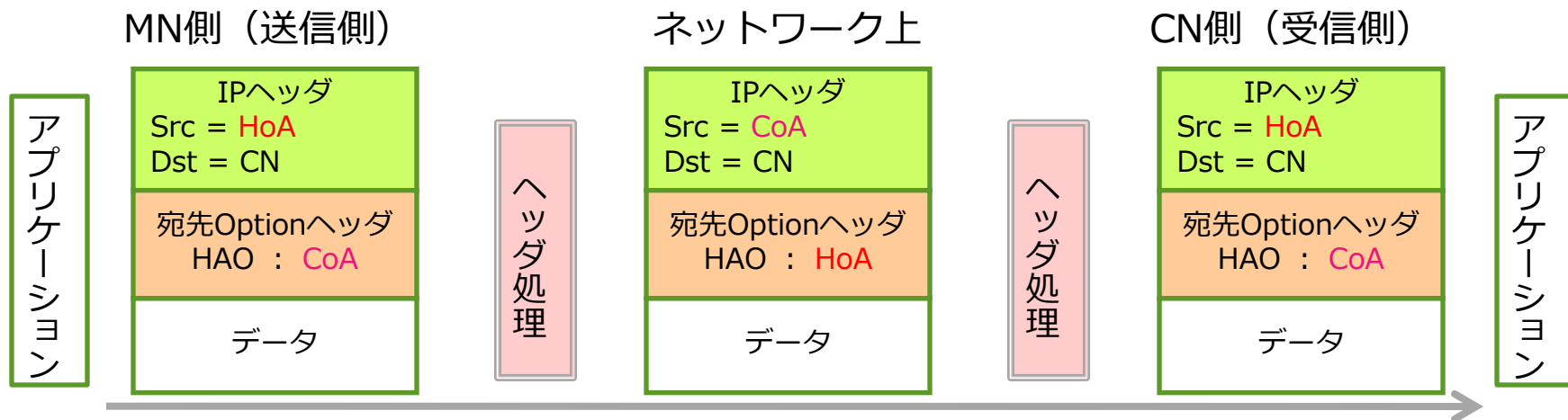
◆宛先オプションヘッダ (ホームアドレスオプション)



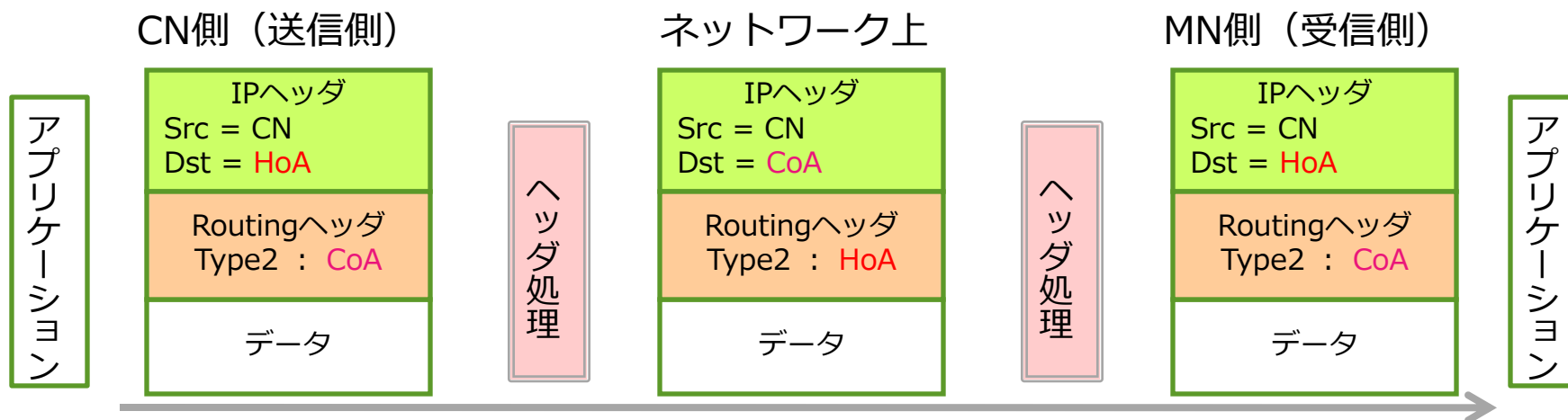
※受信ノードは宛先アドレスをHoAに置き換えて上位層にデータを渡す

1-7-6. 拡張ヘッダを用いた経路最適化

◆MNからCNへの通信（宛先オプションヘッダを利用）



◆CNからMNへの通信（ルーティングヘッダを利用）



※アプリケーションは常にCNとHoAの通信であると認識するため通信が継続される

◆ネットワークのモビリティ

- ルータが移動ノードのように振舞いネットワーク単位の移動を実現
ITS (Intelligent Transport Systems) での利用に期待
自動車は移動するネットワークとなる
- IPv6でのみ利用可能
IPv6の普及が遅れているためIPv4ネットワーク利用の拡張も検討中

◆トラフィッククラス (Traffic Class)

- パケットに優先順位を設定
- Class of Service : CoS
IPv4で定義されていたTOS (Type of Service) と同様なもの

◆フローラベル (Flow Label)

- 発信元にて設定するフローを識別する値
フロー毎のQoS制御
- ルートキャッシングによるパケット転送の高速化
実時間通信の実現など

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

※明確な利用方法や方針などは
まだ決まっていない

◆IPv6のためのDNSレコード

●AAAAレコード

ホスト名からIPv6アドレスへの変換（正引き）のためのレコード
IPv4のAレコードと同じような記述方法

＜記述方法＞

```
$ORIGIN example.com.
```

```
www IN AAAA 2001:db8:cafe:1::80
```

●A6レコード

階層的な名前解決を実現するための正引きレコード
実験的な利用となっており一般的には利用されない

◆IPv6の逆引き用ドメイン

●ip6.arpaドメイン

IPv6アドレスからホスト名への変換のためのドメイン
IPv6アドレスを逆に並べた書式が用いられる

＜記述方法＞

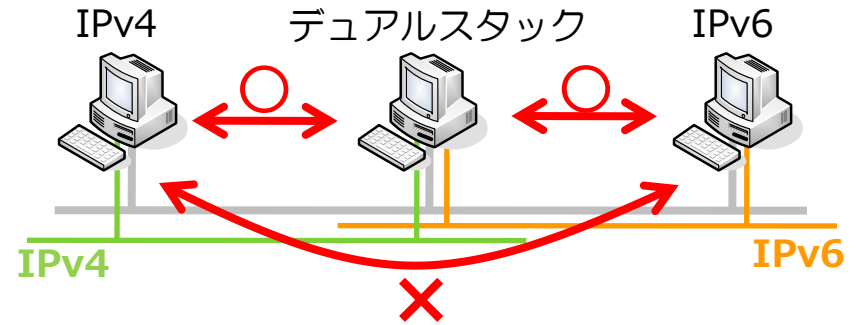
```
$ORIGIN e.f.a.c.8.b.d.0.1.0.0.2.ip6.arpa.
```

```
0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR www.example.com.
```

※0を省略することはできない

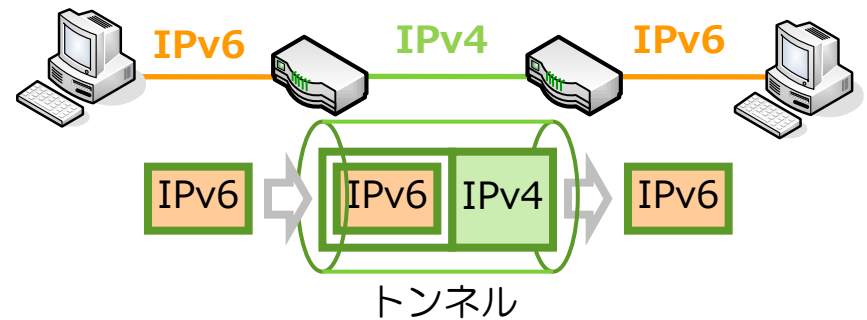
◆デュアルスタック

- IPv4とIPv6双方をサポート
現状のIPv6対応製品のほとんどがデュアルスタック
- 二重の運用が必要



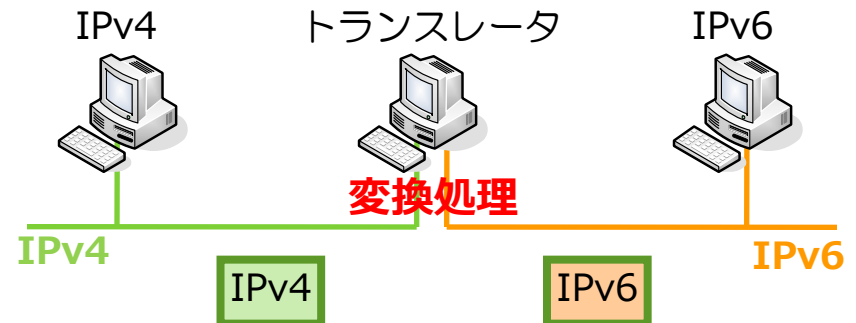
◆トンネリング

- IPv4でカプセル化して通信
- IPv6をIPv4として扱う
VPNと同様の技術
- 自動トンネリング技術
6to4, Teredo, ISATAP



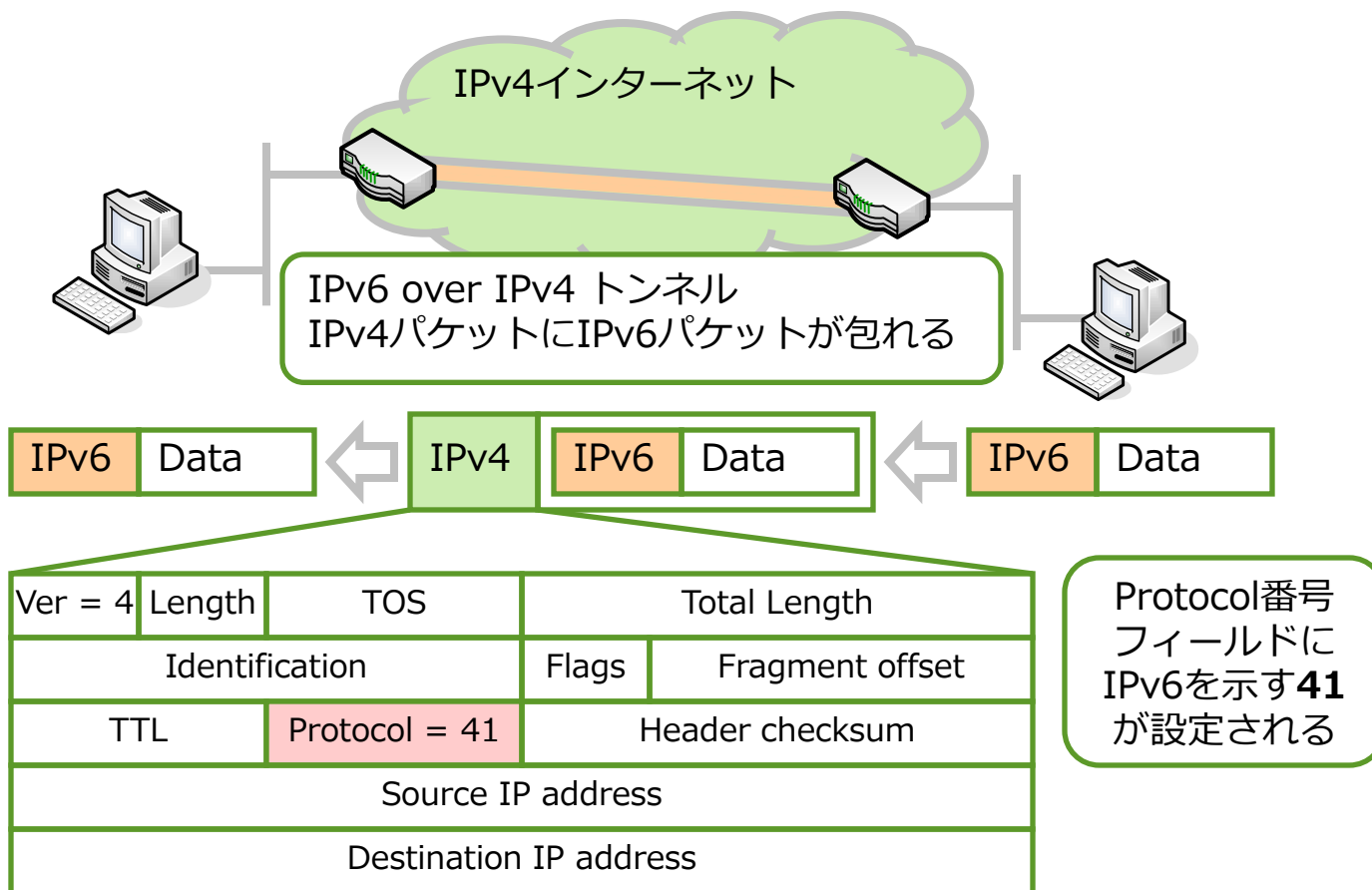
◆トランスレータ

- 通信を仲介する翻訳機
デュアルスタックで構成される
- NATと同様万能ではない
アプリケーションレベルの対応が必要な場合もある



◆固定トンネリングの特徴

- トンネルの両端にて設定を実施
- 拡張性が乏しいが利用するIPv6アドレスに制限なし



◆自動トンネリングの特徴

- 利用するアドレスに制限があるが導入が容易

◆6to4のアドレス形式

[RFC3056]

6to4 TLA 2002	6to4端末の IPv4アドレス	サブネットID	インターフェイスID
16ビット	32ビット	16ビット	64ビット

- ・トンネル接続とIPv6アドレス割り当てを同時に実現

◆Teredoのアドレス形式

[RFC4380]

Teredoプレフィックス 2001:0000	Teredoサーバの IPv4アドレス	フラグ	隠蔽した ポート番号	隠蔽したNATの IPv4アドレス
32ビット	32ビット	16ビット	16ビット	32ビット

- ・NATトラバーサルをIPv6で実現する技術

※NATトラバーサル： NATの内側への到達性を提供する技術 隠蔽： all 1とのXOR

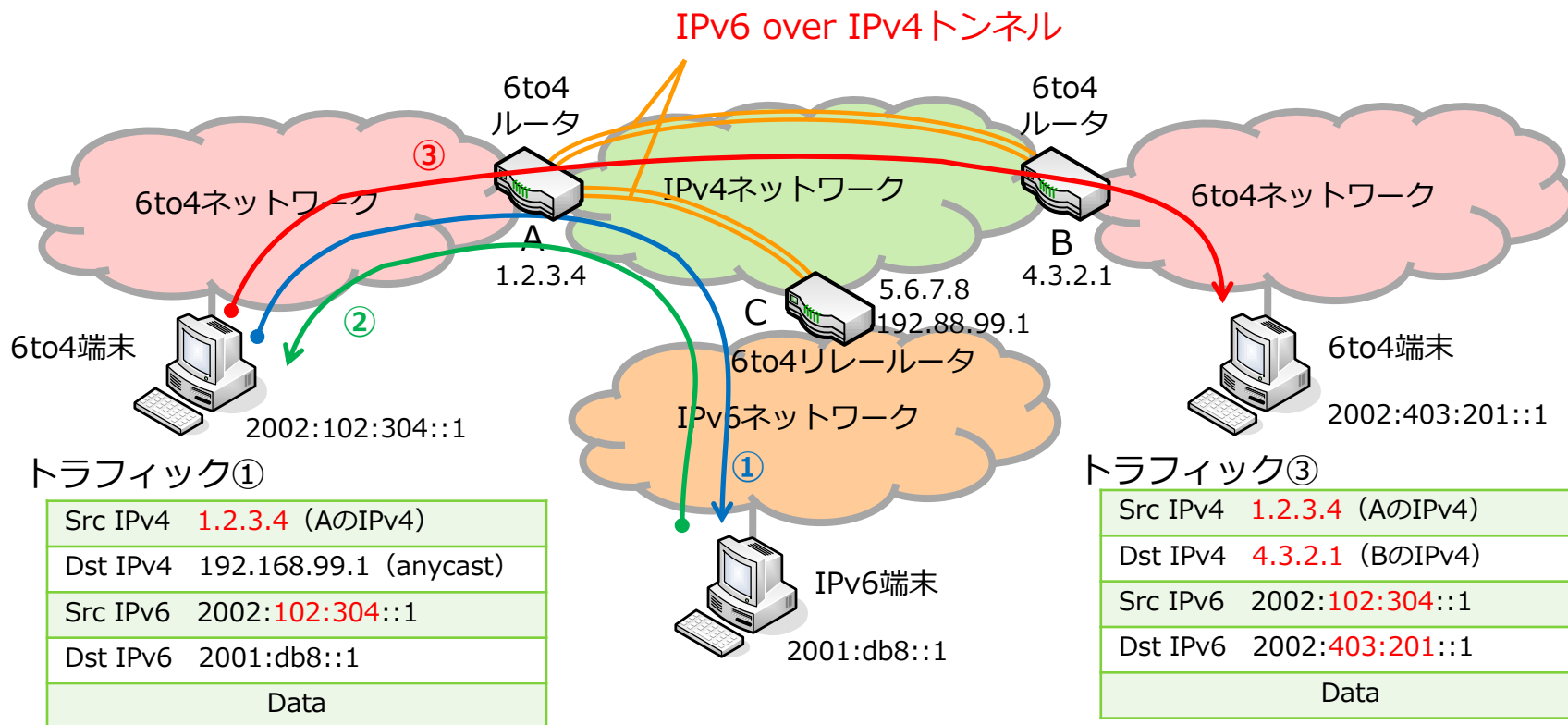
◆ISATAPのアドレス形式

[RFC4214]

サイトプレフィックス (一般的なIPv6アドレスのプレフィックス)	ISATAP ID 0000:5efe	ISATAP端末の IPv4アドレス
64ビット	32ビット	32ビット

- ・企業イントラネット内でのトンネリング技術

1-9-3. 6to4の仕組み

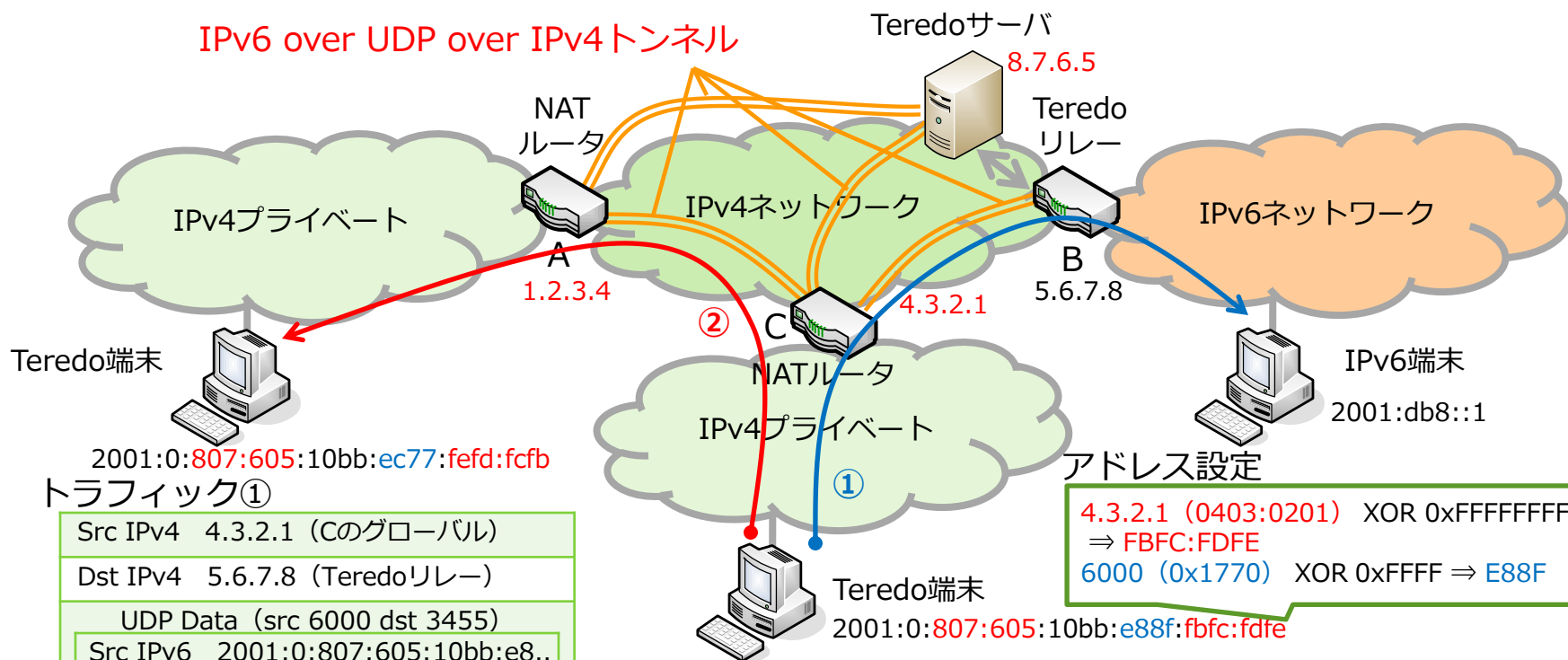


トラフィック②

Src IPv4	5.6.7.8 (CのIPv4)
Dst IPv4	4.3.2.1 (BのIPv4)
Src IPv6	2001:db8::1
Dst IPv6	2002:403:201::1
Data	

トラフィック①：6to4端末からIPv6端末への通信
 192.88.99.1は6to4リレールータの**エニーキャストアドレス**
 トラフィック②：IPv6端末から6to4端末への通信
 6to4リレールータのIPv4アドレスとIPv6端末アドレスに関連はない
 6to4リレールータはネットワーク上に複数存在し経路制御プロトコルにより最適なものが選択される（行き帰りで経路が同じとは限らない）
 トラフィック③：6to4端末から6to4端末への通信
 6to4アドレスから6to4ルータのアドレスを得ることができる

1-9-4. Teredoの仕組み



アドレス設定

4.3.2.1 (0403:0201) XOR 0xFFFFFFFF
⇒ FBFC:FDFE

6000 (0x1770) XOR 0xFFFF ⇒ E88F

トラフィック①

Src IPv4	4.3.2.1 (Cのグローバル)
Dst IPv4	5.6.7.8 (Teredoリレー)
UDP Data (src 6000 dst 3455)	
Src IPv6	2001:0:807:605:10bb:e8..
Dst IPv6	2001:db8::1
Data	

トラフィック②

Src IPv4	4.3.2.1 (Cのグローバル)
Dst IPv4	1.2.3.4 (Aのグローバル)
UDP Data (src 6000 dst 5000)	
Src IPv6	2001:0:807:605:10bb:e8..
Dst IPv6	2001:0:807:605:10bb:ec..
Data	

アドレス設定

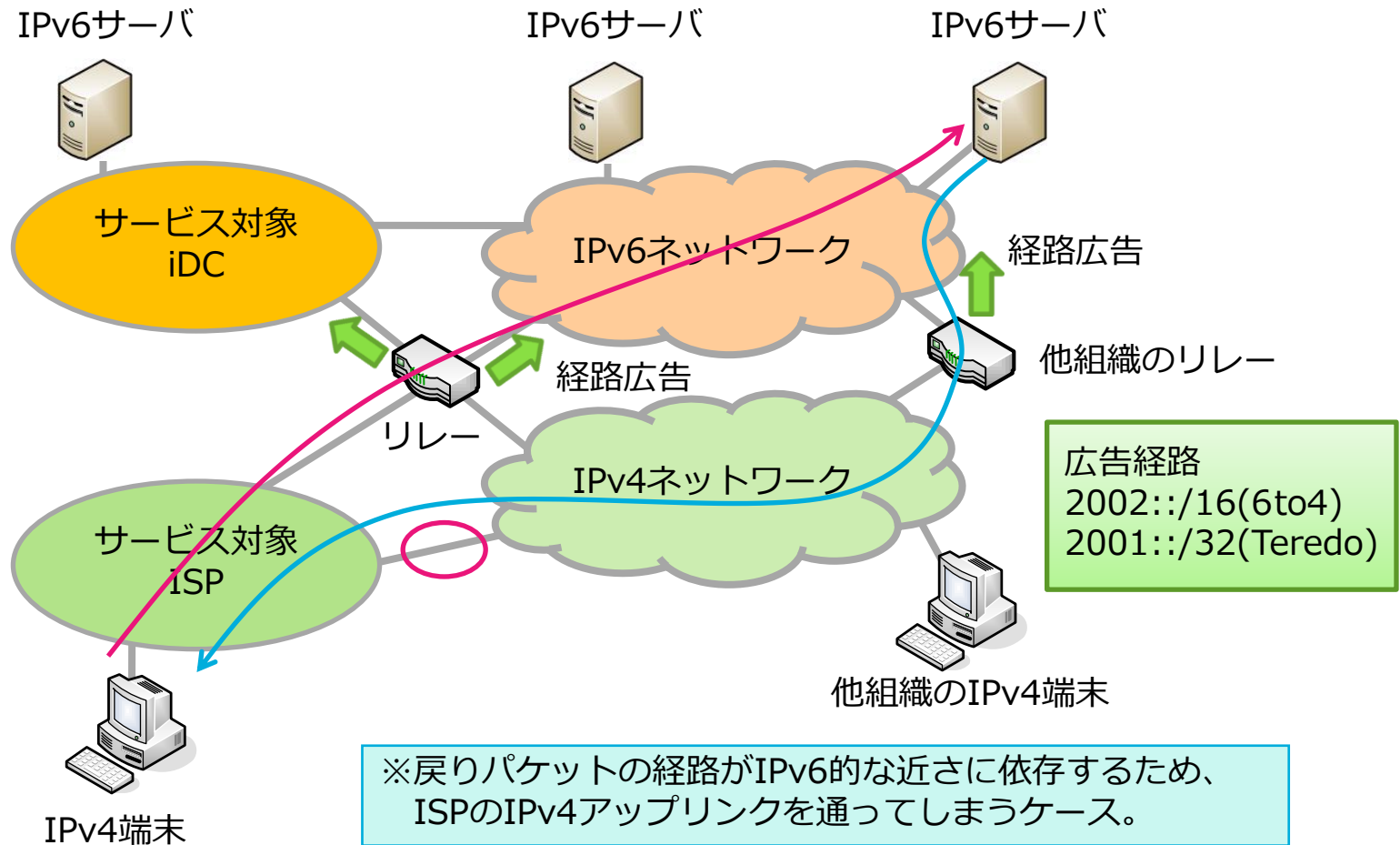
TeredoサーバのUDP3455宛に通信しIPv6アドレスを取得
 アドレスにはNATルータのIPv4アドレスとポート番号が隠蔽して含まれる

トラフィック①： Teredo端末からIPv6端末への通信
 Teredoリレーの宛にIPv6パケットを内包して送信
 TeredoリレーにてIPv6通信が取り出されIPv6ネットワークへ転送

トラフィック②： Teredo端末間の通信
 Teredoアドレスから得られるNATアドレスと外部ポート番号へ通信すると
 NATルータでは対応ポート番号宛のパケットをTeredo端末に転送する
 NATルータ間ではトンネルが形成されたような通信を行う

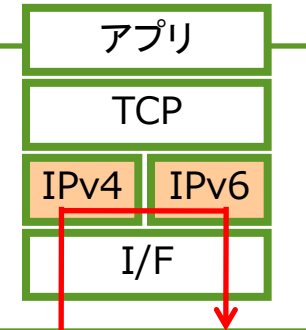
◆ 経路制御が困難

- サービス対象にのみ提供することが難しい



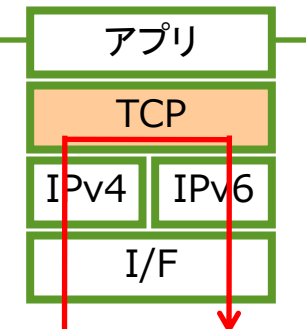
◆ヘッダ変換方式

- IPv4ヘッダとIPv6ヘッダの相互変換を実現
IPv4でのNATに似た技術
NAT-PT (RFC2766) など ※現状Historical扱い
- 処理のオーバーヘッドは比較的小さいが制約がある



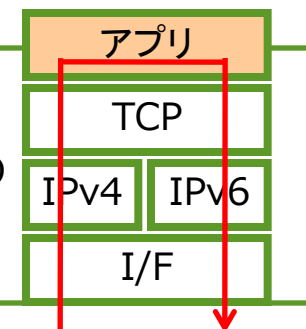
◆TCPリレー方式

- トランスポート層 (TCPセッション) での中継方式
TRT (RFC3142) など
TCPコネクションが独立となる
- ヘッダ変換方式よりも処理が大きいが制約は少ない

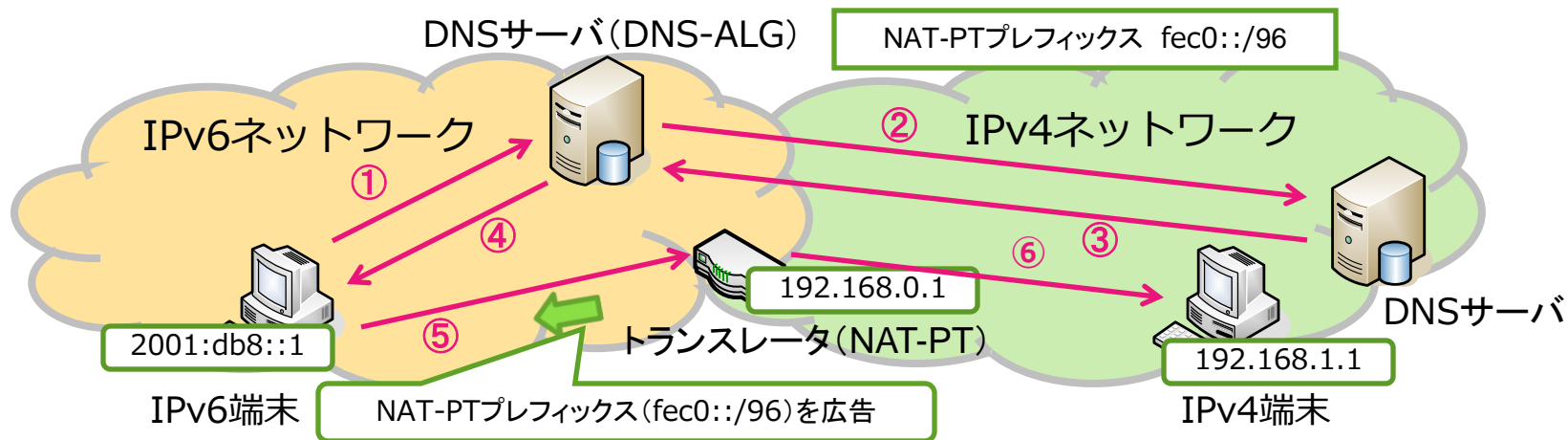


◆アプリケーションレベルゲートウェイ (ALG) 方式

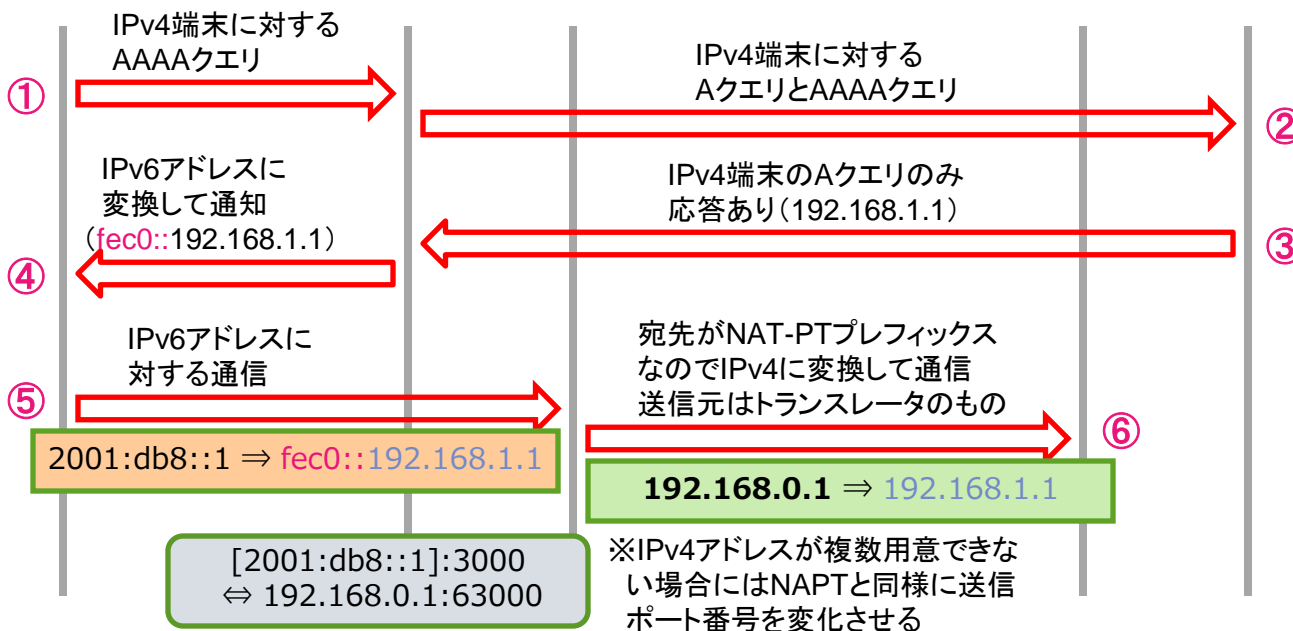
- アプリケーションによる中継方式
- 処理のオーバーヘッドが一番大きくアプリケーション毎の対応が必要になるが相互接続性を完全に確立できる



◆IPv6端末がIPv4端末に通信する場合



- ・名前解決
DNS-ALGにて
IPv6アドレスに
変換して通知
- ・通信開始
トランスレータ
にてプロトコル
変換を実施して
パケット中継



2. IPv6の現状

内容：IPv6の現状を確認

2-1. IPv6の普及度

2-2. IPv6によるサービス

2-3. 機器の対応状況

2-4. Windowsでの挙動

2-5. 現在の論点

2-1. IPv6の普及度

◆IPv6アドレスの利用状況

- アドレスブロックの割り当ては加速気味
欧米諸国でのIPv6アドレス取得が近年伸びている
/19などの大きなアドレス割り当ても発生
- 広告されている経路数はようやく1000プレフィックスを超えた
IPv4の経路数（約27万）と比べるとかなり少ない

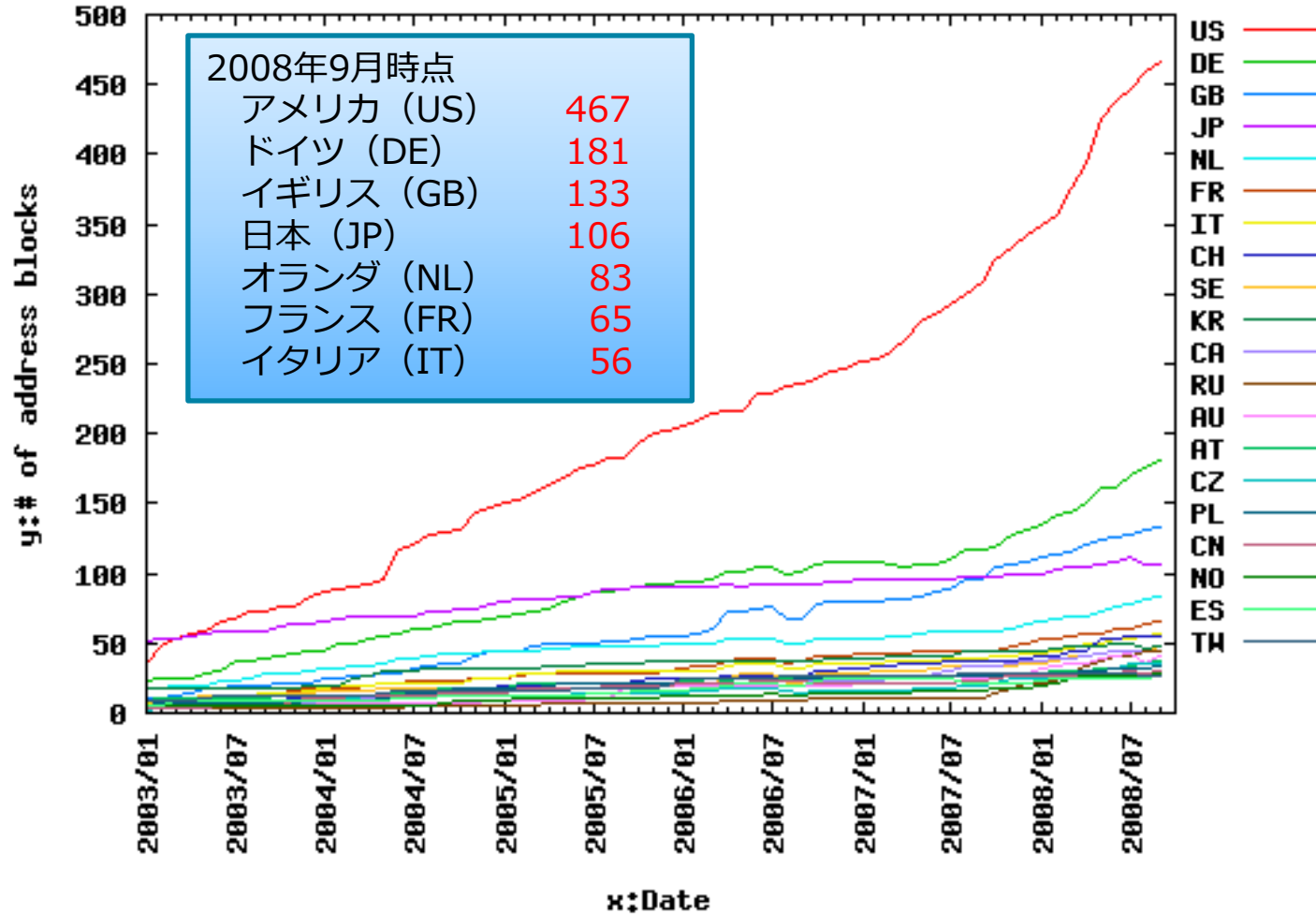
◆IPv6対応製品

- Gold Logoでのアメリカの対応製品の登録が伸びている
- IPv6 Ready Logo Program
IPv6対応機器の相互接続性を認定するプログラム
Phase 1 (Silver) : 基本的なIPv6仕様の準拠
Phase 2 (Gold) : RFCでのMUST/SHOULDの仕様全てに準拠

◆DNSにおけるIPv6アドレス登録（JPドメイン対象）

- NSレコードが登録されたドメインは4000を超えたところ
IDCのIPv6対応による影響が観測されるくらい小さい
- MXレコードの登録はほぼ横ばい
実際の利用まで至っていない現状

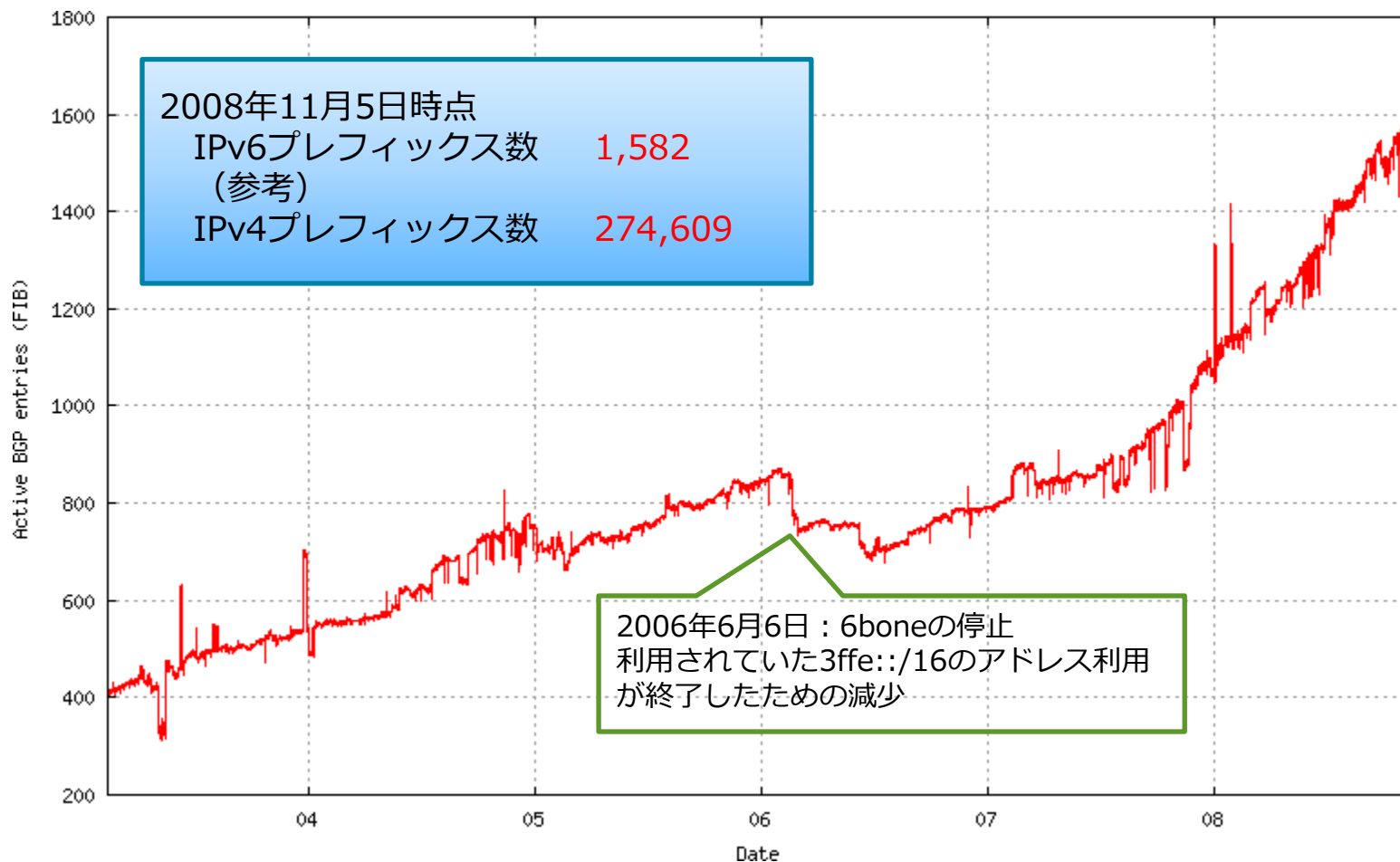
アドレスブロック単位の割り当て数（国別）



Copyright (C) Internet Association Japan

<http://v6metric.jp/html/st01/08.html>

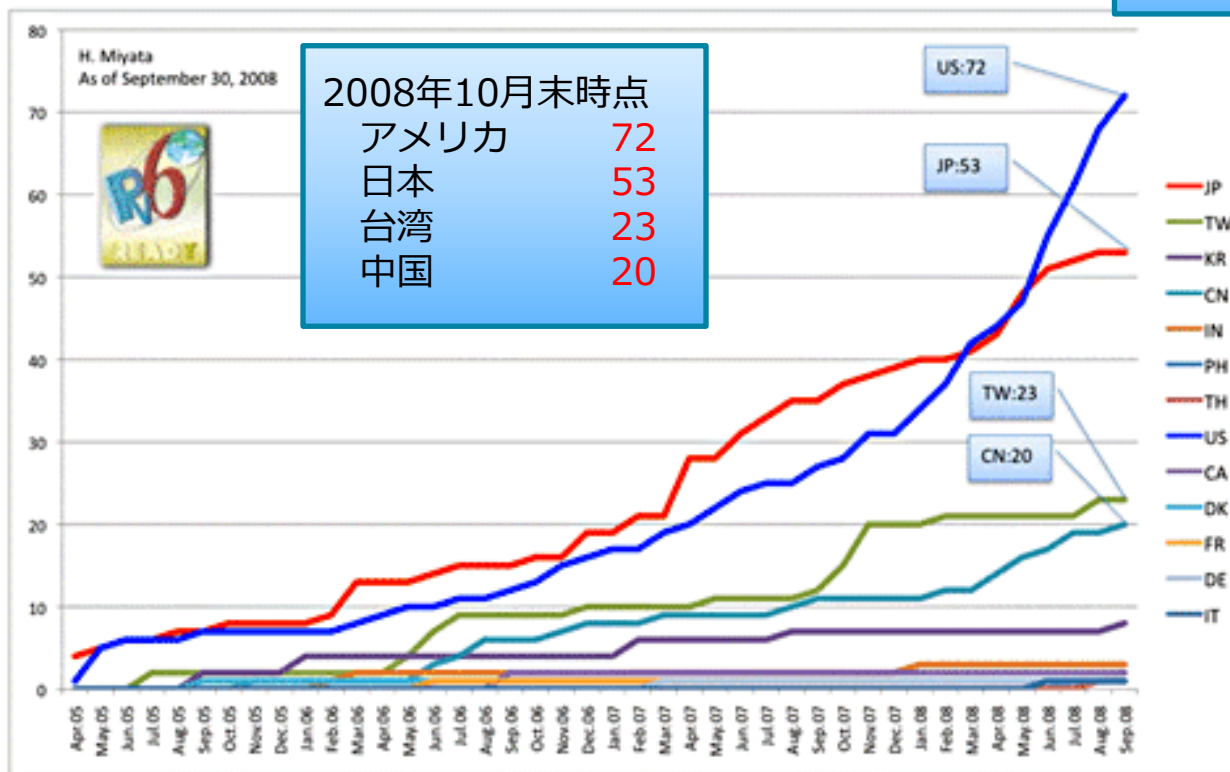
AS2.0におけるIPv6の経路数 (BGP4のFIBより)



<http://bgp.potaroo.net/v6/as2.0/index.html>

IPv6 Ready Logoの登録機器数（国別）

Phase 1 登録数 370
Phase 2 登録数 235

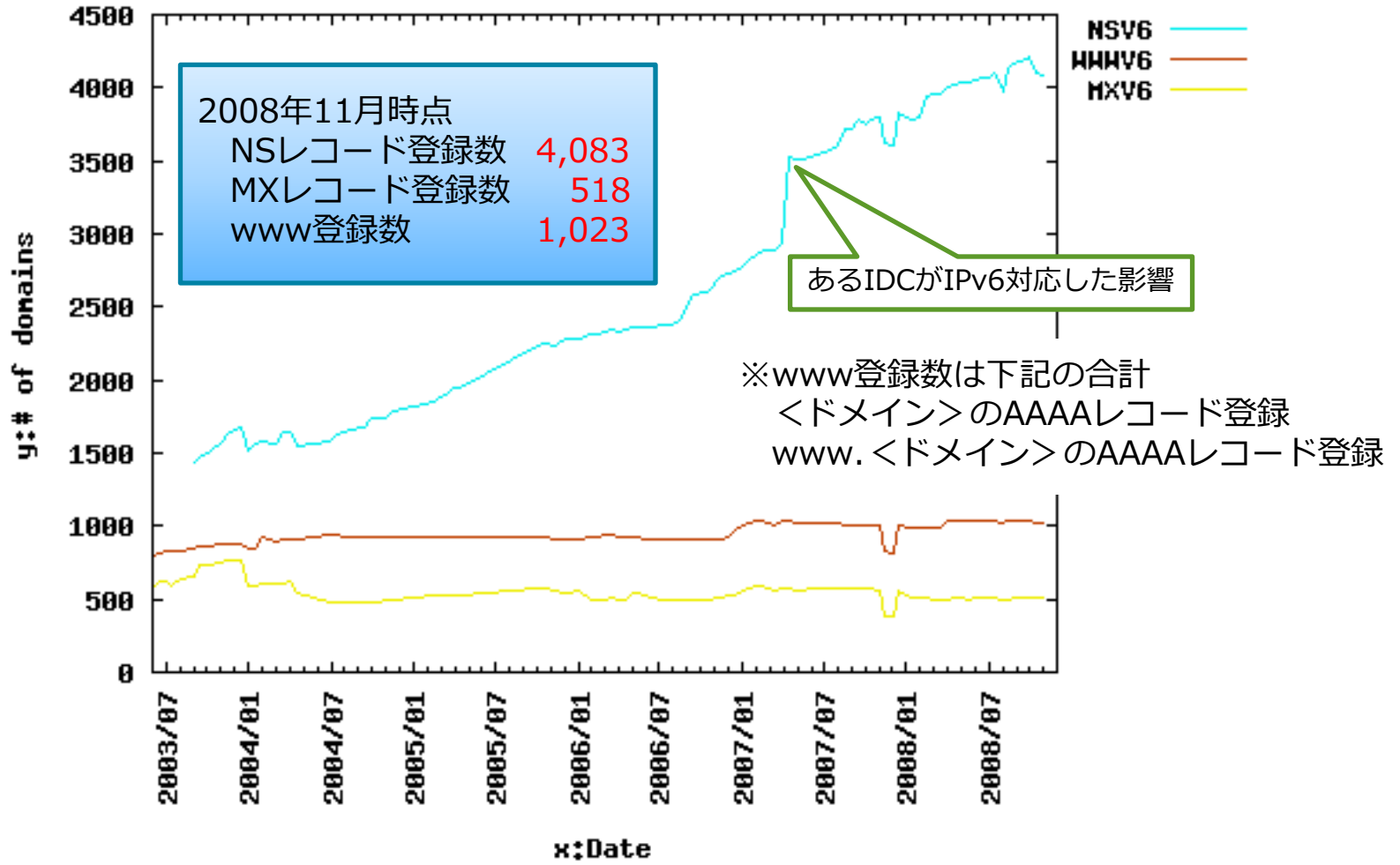


2008/10/22

IPv6 Promotion Council - Certification WG
Copyright© Yokogawa Electric Corporation

<http://www.v6pc.jp/jp/spread/index.phtml>

JPドメインにおけるIPv6レコードの登録数



Copyright (C) Internet Association Japan

<http://v6metric.jp/html/st04/04.html>

◆IPv6接続サービス

サービス名	サービス内容／割り当てプレフィックス
IJ IPv6トンネリングサービス http://www.ij.ad.jp/service/IPv6/	固定のトンネリング接続で/48のプレフィックスを付与
OCN IPv6 http://www.ocn.ne.jp/ipv6/	L2TPによるトンネル接続環境の提供 /64のプレフィックスを2ブロック（固定と非固定）付与
KDDI IPv6トンネリングサービス http://www.kddi.com/business/ipv6_tunneling/	/48を割り当てる固定トンネリング接続 独自取得したアドレス利用も可能
Nifty @nifty IPv6接続サービス http://www.nifty.com/ipv6/	ADSLサービス上でのデュアルスタックサービス /64のプレフィックスを付与
フリービット Feel6接続サービス http://start.feel6.jp/	DCTPによる動的トンネリング設定を利用 /64のプレフィックスを付与する無料サービス
NTT東日本 フレッツ・光 http://flets.com/dotnet/ NTT西日本 フレッツ・光プレミアム http://flets-w.com/hikari-p/	地域IP網に閉じたIPv6ネイティブ接続サービス /64がルータ広告により付与 <u>IPv6マルチキャスト</u> を利用した映像配信サービスなどを 提供可能なネットワークを構成

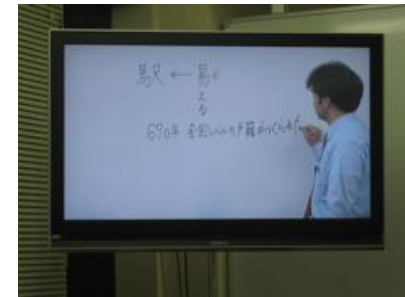
◆NTTフレッツ内IPv6サービス

- 映像配信（IPv6マルチキャストを利用したサービス）
フレッツ・テレビ, ひかりTV, ギャオネクスト, スカパー！光
- 付加サービス（双方向通信を生かしたサービス）
フレッツ・ドットネット, フレッツ・v6アプリ

◆IPv6マルチキャスト放送システム (i-InproV6)

- 塾の遠隔授業などに利用
衛星配信と比べコストが最大で1/10に
 - ・イニシャル：数億円⇒2,000万円弱
 - ・ランニング：1,000万円/月⇒100万円/月有名講師が全校舎を担当
レベルを均一化、1授業当たりの利益向上

遠隔授業風景



<http://becare.co.jp/service/case01.html>

◆緊急地震速報配信サービス (OCN)

- 気象業務支援センターの緊急地震速報を配信
緊急性、リアルタイム性、配信効率性

受信端末/アプリケーション



<http://www.ntt.com/jishinsokuho/index.html>

◆コンビニ店舗への一括配信 (FamilyMart)

- 6,000店舗をデュアルスタック化
- 衛星からブロードバンド&マルチキャストへ
- キオスク端末への新商品キャンペーン、従業員向けマニュアル等の大容量ファイル一括配信

キオスク端末 (Famiポート)



3-3. 機器の対応状況

◆OS/ルータ/スイッチ

- Windows : XP (非サポート) , Mobile2003, CE.NET, Vista
- Mac OS X, Linux, BSD系OS
- バックボーン系ルータはほぼ対応済みで一部の家庭用も対応
Cisco, Juniper, Alaxala, Yamaha, NEC, コレガなど
※ フレッツ向けの「IPv6対応」はIPv6ブリッジ機能なので注意

◆ネットワーク機器

- 負荷分散装置 : F5(BIG-IP)
- Firewall : Checkpoint(VPN-1/FireWall-1), Juniper(Netscreen)
- NW管理 : HP(OpenView), 日立(JP1)など
- 計測器 : 東陽テクニカ(Smartbits)、Agilent(N2X)など

◆アプリケーション

- アンチウィルス : トレンドマイクロ (ウィルスバスター)
- サーバアプリケーションのほとんどが対応済み
参考 : Current Status of IPv6 Support for Networking Applications
http://www.deepspace6.net/docs/ipv6_status_page_apps.html

2-4. Windowsでの挙動

◆IPv6対応OS Windows Vista

- 代表的なコンシューマOSがIPv6に完全対応
GUIによるIPv6設定
IPv4/IPv6を意識させないAPI
- ほとんどのWindowsコンポーネントがIPv6対応に
IPv6 onlyは容易 (IPv4 onlyは基本的に不可)



◆IPv6デフォルト有効による影響

- DNSクエリ関連
AレコードとAAAAレコードの名前解決のためクエリが増加する
名前解決の優先順位は実装依存
- 自動トンネリングプロトコル機能
6to4やTeredoがデフォルトで有効
- IPv6利用の認識が必要
ルータ広告受信で即IPv6利用が可能

2-4-1. DNSの挙動

◆DNSクエリの増加

- デュアルスタックによるDNSクエリの倍増
Aクエリ+AAAAクエリ=約2倍
- DNSサフィックス付加機能
OSにより付加（DHCPによるドメイン名等）
検索エンジンにより付加（Webブラウザ）

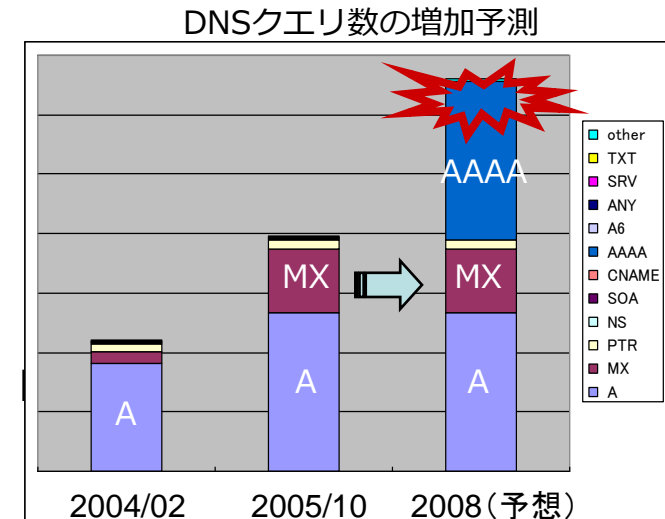
「IPv6端末OSにおけるIPv6対応・IPv6機能活用ガイドライン」より

◆壊れたAAAAクエリの応答対応

- AAAAクエリにIPv4アドレスを返す実装が存在
IPv4アドレスはOSレベルでは受け入れる実装
⇒アプリケーションで無視する設定が必要（RFC4074参照）

◆名前解決の順序（XPと異なるVistaの挙動）

- AAAAクエリの抑制
グローバルIPv6アドレスが付与されない限り利用しない
※Teredoアドレスを除くグローバルアドレス
- Aクエリを優先的に実施
Aクエリの応答結果をAAAAクエリに利用
 - ・Aクエリの応答時間によりAAAAクエリの処理待ち時間を決定
 - ・AクエリがNXDOMAINならAAAAクエリは出さない



2-4-2. 自動トンネリング機能

◆6to4アドレスの自動設定

- グローバルIPv4アドレスを持つと設定される
デフォルト設定の6to4サーバ：**6to4.ipv6.microsoft.com**
6to4エニーキャストアドレス（192.168.99.1）を持っている
⇒ ネットワーク的に近いものが勝手に選ばれる
- 普通にIPv6インターネットと通信が可能
RAなどによるIPv6アドレスが付与された場合には利用されない
IPv6のみの通信相手にしか利用されない（IPv4を優先）

※宛先/始点アドレス選択ルール（RFC3484）のルールに因る動作

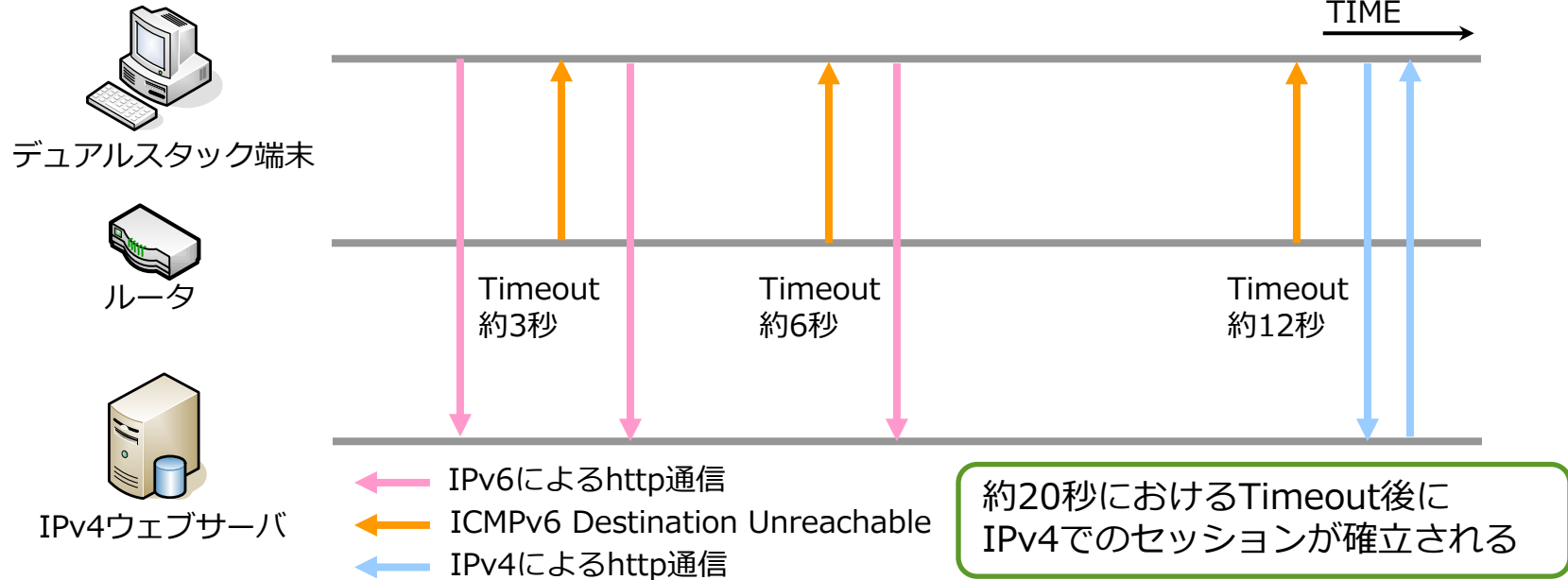
◆Teredoアドレスの自動設定

- NAT配下のセグメントに接続で設定
デフォルト設定のTeredoサーバ：**teredo.ipv6.microsoft.com**
Windowsファイアウォールが有効な場合のみ設定される
- Teredoリレーを介したIPv6通信が可能
自身から発信しない限り有効なインターフェイスにならない
IPv6の名前解決は行われない
⇒ 直接IPv6アドレス指定する必要あり

◆RA受信による脅威

- RA受信によりIPv6を利用した通信が可能に
- IPv4のみのセグメントでもIPv6アドレスが付加
到達性のないRAでもIPv6で通信を試みるため時間がかかる
⇒ TCPフォールバック問題
- 悪意のあるRAによるパケット収集の危険
誰でも簡単にデフォルトルートになれる事が問題

◆TCPフォールバック



2-5. 現在の論点

◆トランスレータの仕様

- NAT-PTが歴史的扱いになったため代わりとなる技術の議論
IVI, NAT64, sNAT-PTなど多数議論中

◆RAに関する議論

- ルータ広告のMフラグとOフラグの扱い
- 不正なルータ広告の扱いに関する議論 (RA Guard)

◆拡張ヘッダに関する議論

- 断片化ヘッダの問題 (overlapping fragments)
- 拡張ヘッダの標準フォーマット

◆その他の議論

- DHCPv6における新しいオプション
- IPv6のCPEルータに対する要求条件
- IPv6複数アドレス選択およびRFC3484の改訂
デフォルトルールへのULA追加など
- トンネルプロトコルのセキュリティに関する議論