

IPv6入門

NTT情報流通プラットフォーム研究所

唐澤圭

kei@syce.net



ブロードバンドで、未知の自由へ。

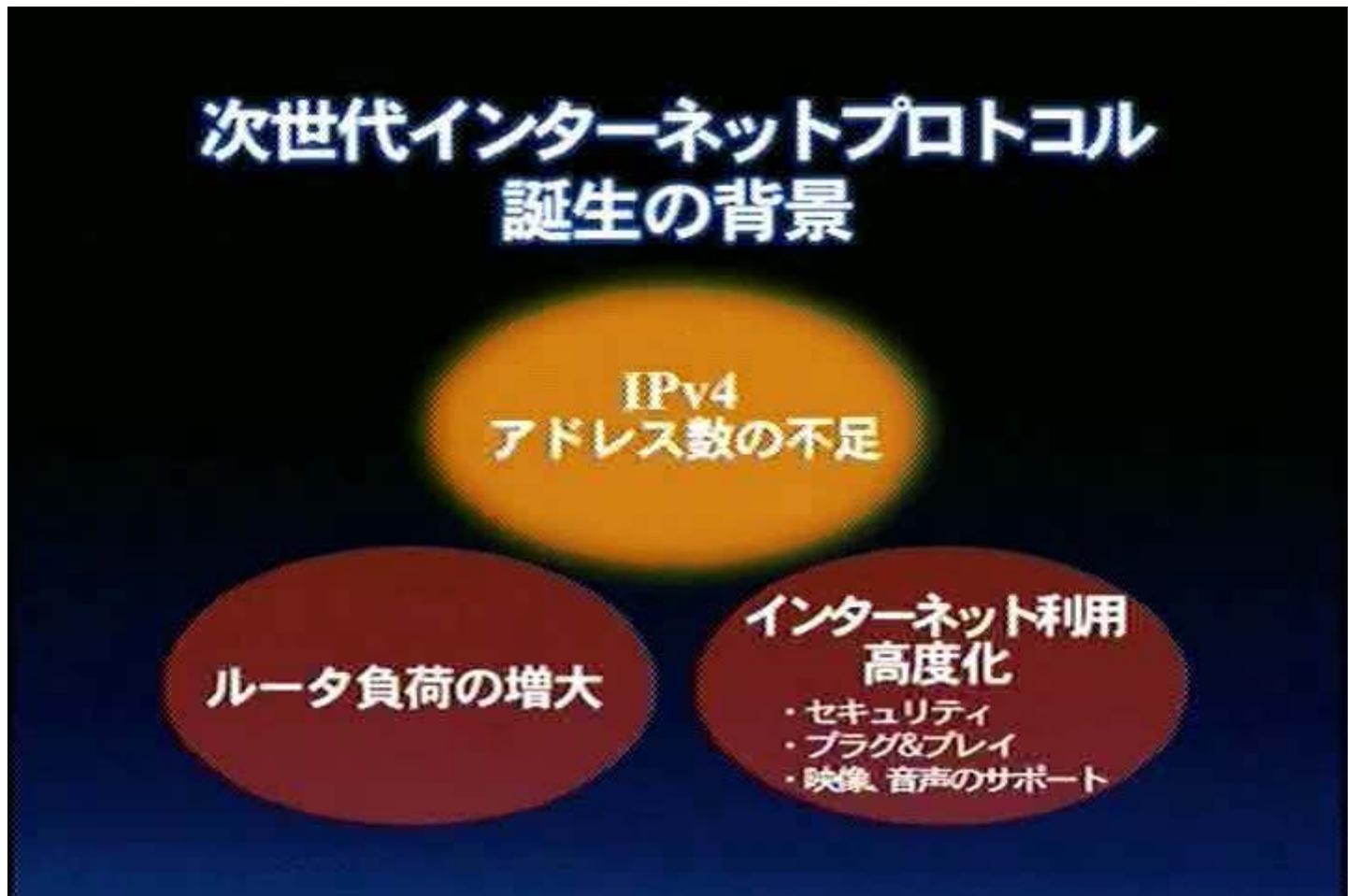
本日の内容

- IPv6のこれまで
 - 誕生の歴史
 - 基本的仕様と機能
 - 拡張的仕様と機能
- IPv6のこれから
 - 関連する新しい仕様
 - ユビキタス・ネットワークの話

IPv6入門ビデオ



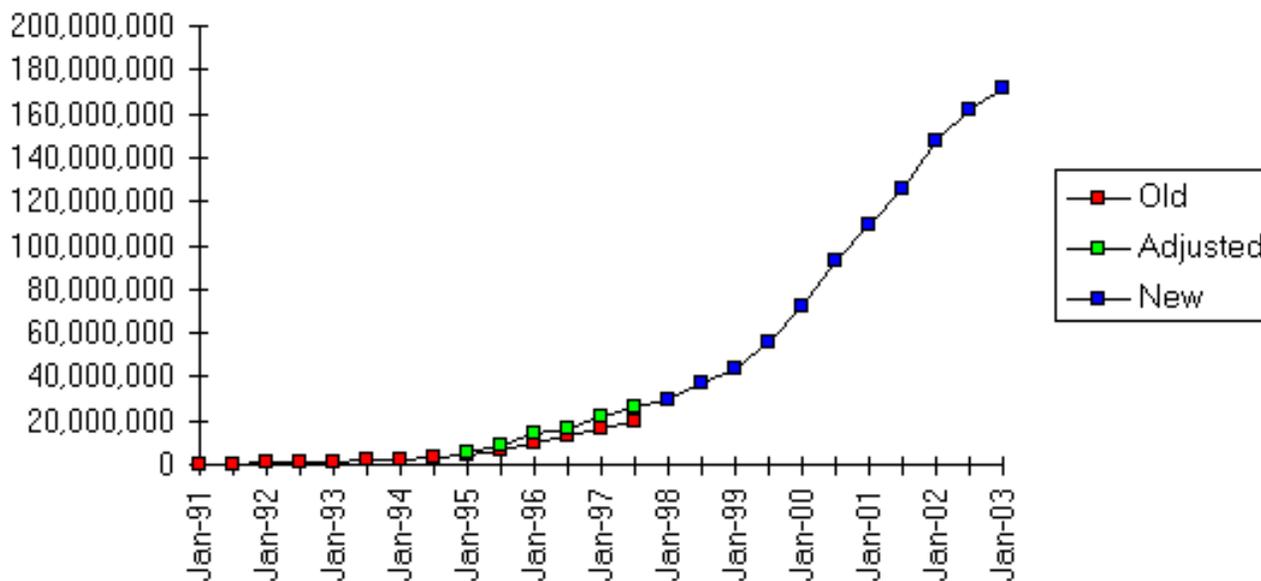
IPv4の問題点 その1



アドレス数の不足

○ インターネット・ホスト数の急増

Internet Domain Survey Host Count

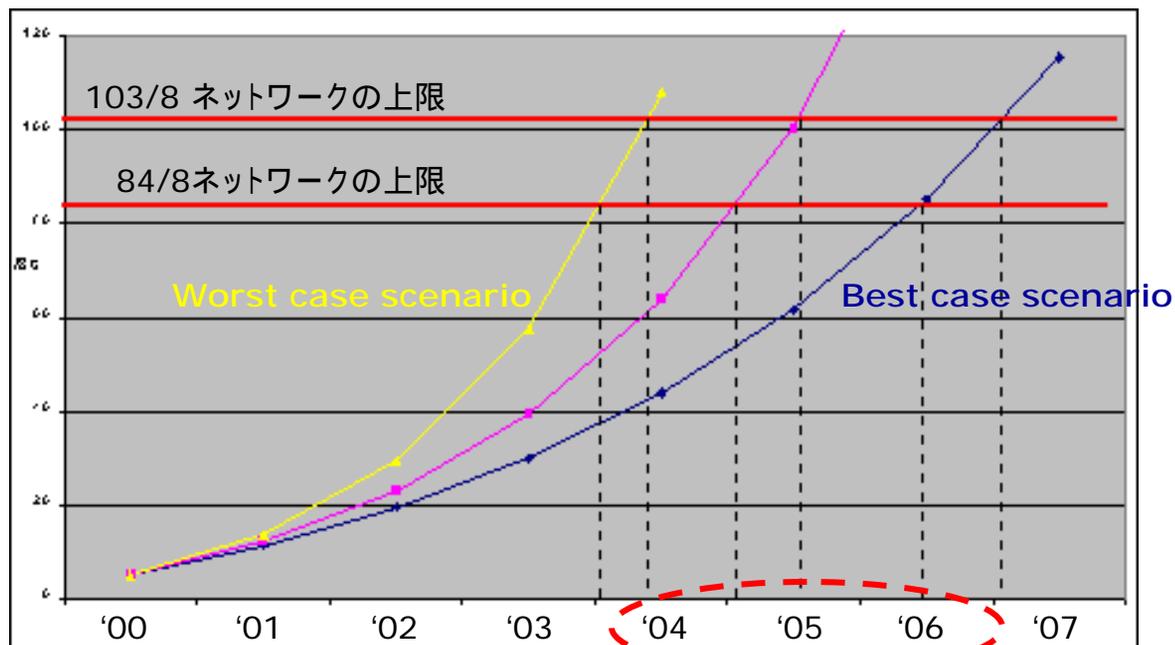


Source: Internet Software Consortium (www.isc.org)

アドレス不足の深刻さ

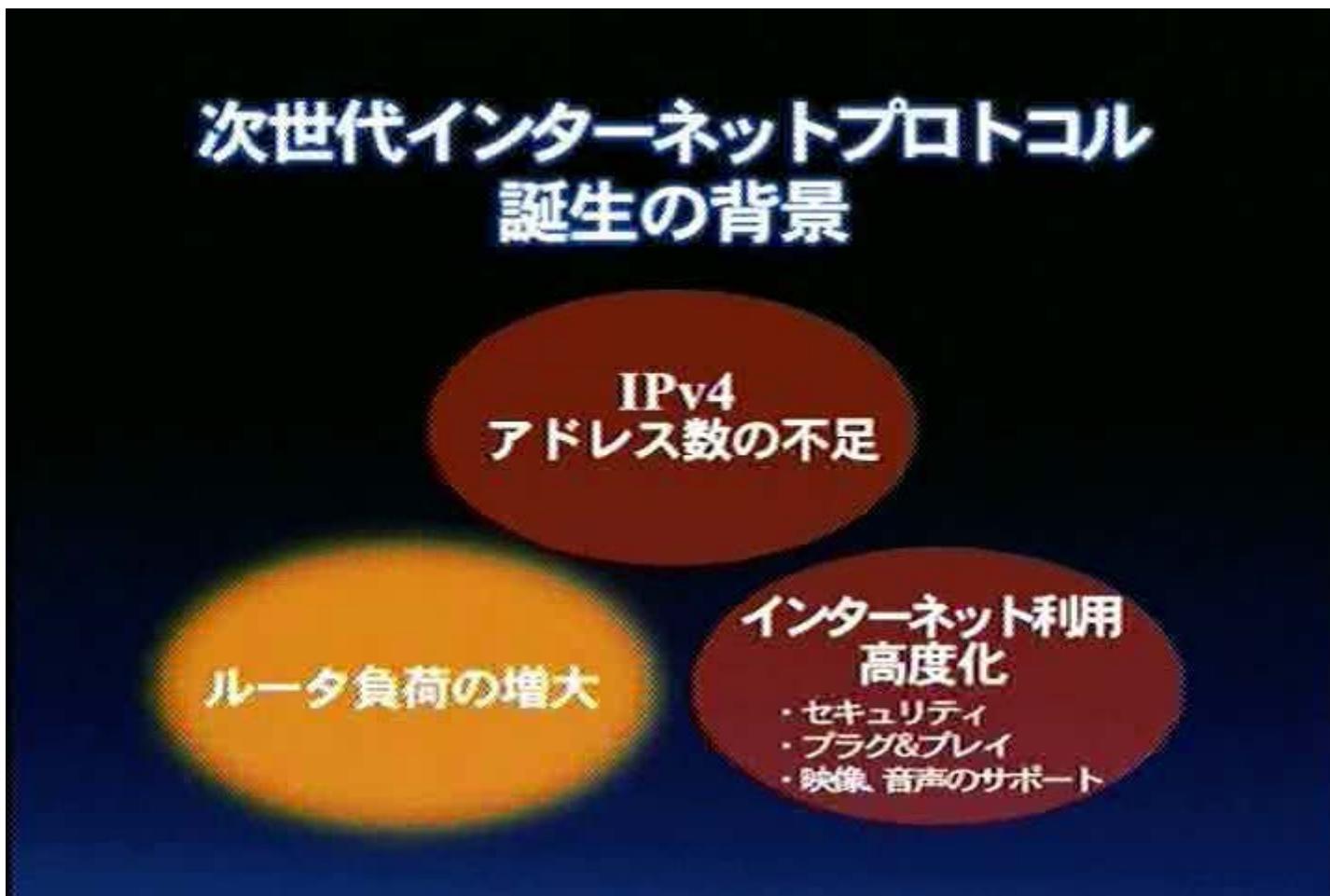
○ アドレスの寿命予測

IPv4 Address Exhaustion (ICANN資料から引用)



2005年ごろにはかなり深刻に

IPv4の問題点その2

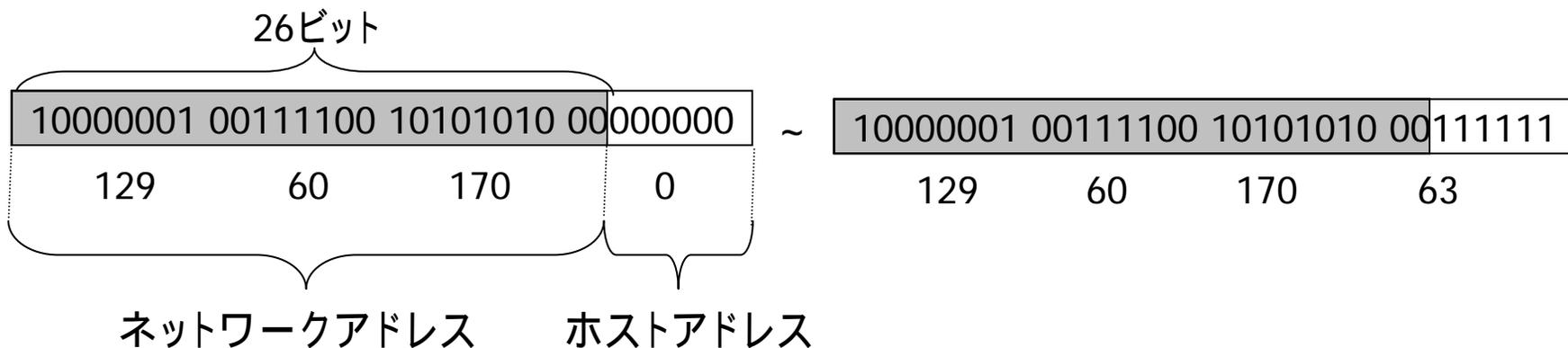


ルータ負荷の増大

- IPv4アドレス利用数増加の副作用
 - IPアドレス割当てルールの変更
 - 未使用アドレスが多くなる”クラスB”からホスト数見合った複数の”クラスC”の割り当てに変更
 - 短期的対策
 - CIDR(Classless Inter-Domain Routing: RFC1519)
 - アドレスの階層的な割当てと経路集約
- 抜本的対策が必要**

CIDR

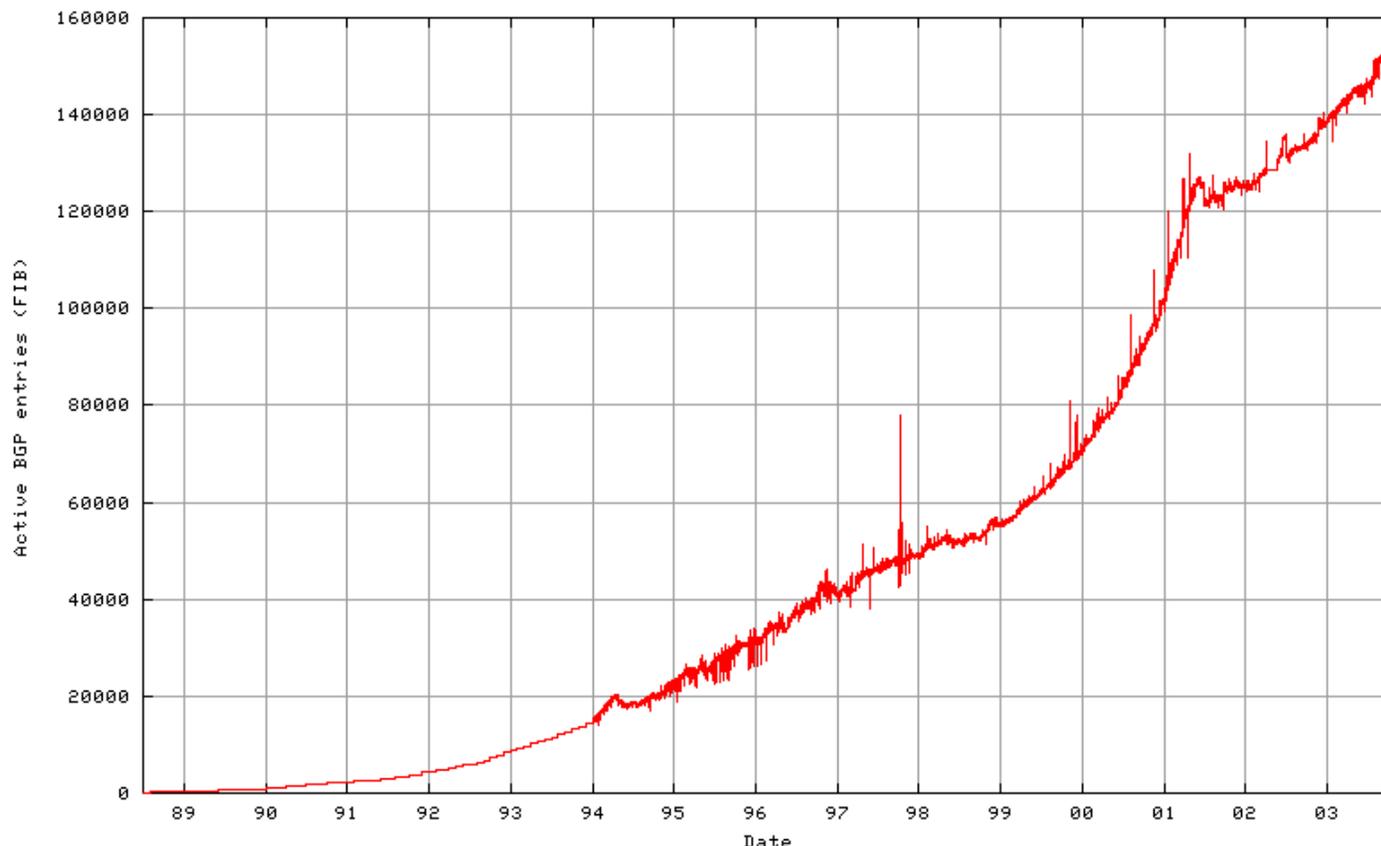
- IPアドレスの効果的な割当てのためCIDRを使用
 - 任意のビット単位でNWアドレスとホストアドレスに区切る
- /20なら4096個のホスト、/26なら64個のホスト
- 例 . 129.60.170.0/26のIPアドレスの場合



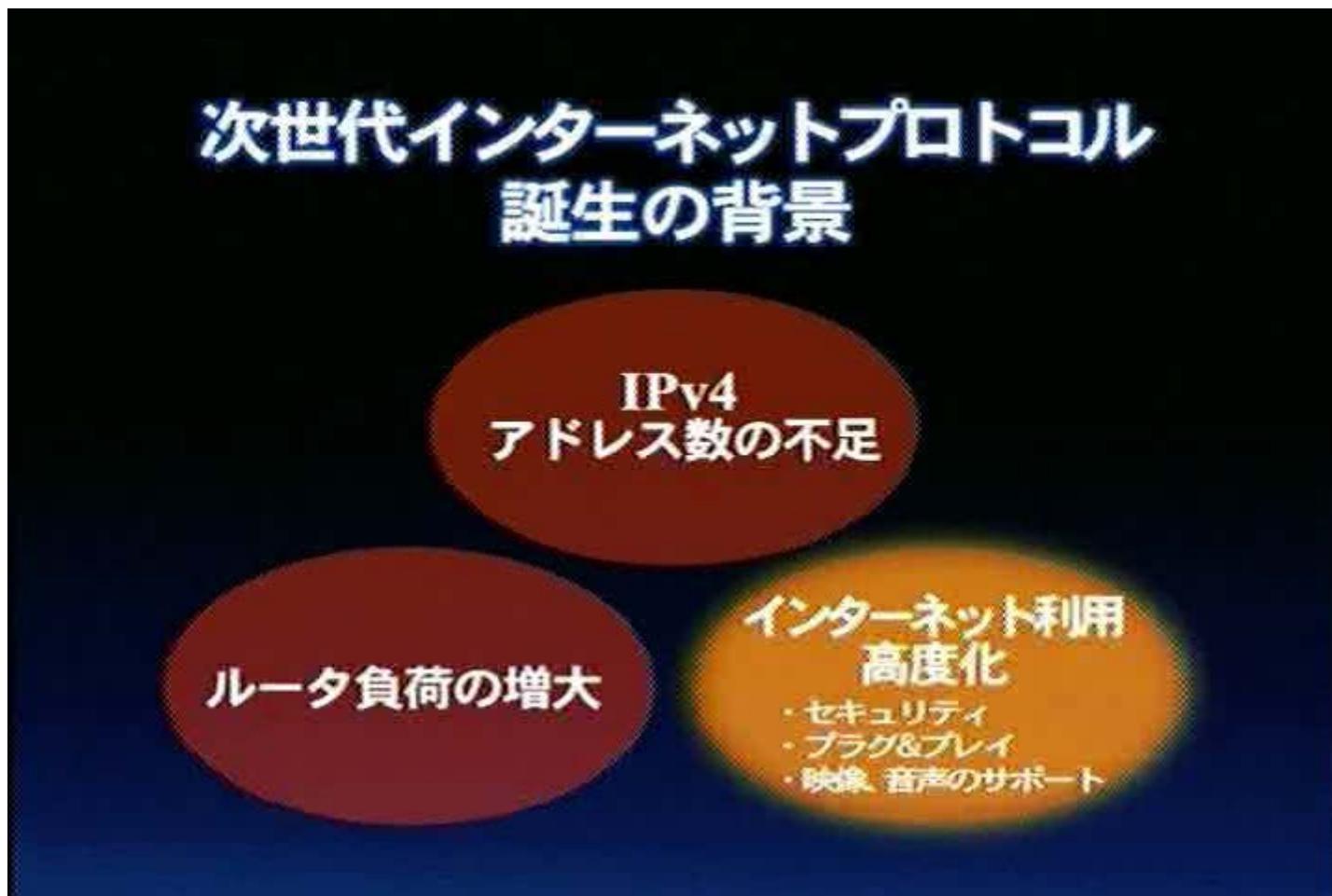
- 後に129.60.170.64/26を割り当てた場合
129.60.170.0/25のように経路集約可能

インターネット経路数の増加

○ BGP Table Data @ Oct 31 2003



IPv4の問題点その3



インターネット利用形態の多様化

○ プラグ&プレイ

- 誰でも簡単に使えるような、ネットワーク環境の自動設定機能

○ セキュリティ

- どんなことにも安心して使えるような、ネットワーク環境(IPレベル)の安全性保証機能

○ 映像、音声のサポート

- 多様なアプリケーションを快適に使えるような、ネットワークの品質確保機能

本日の内容

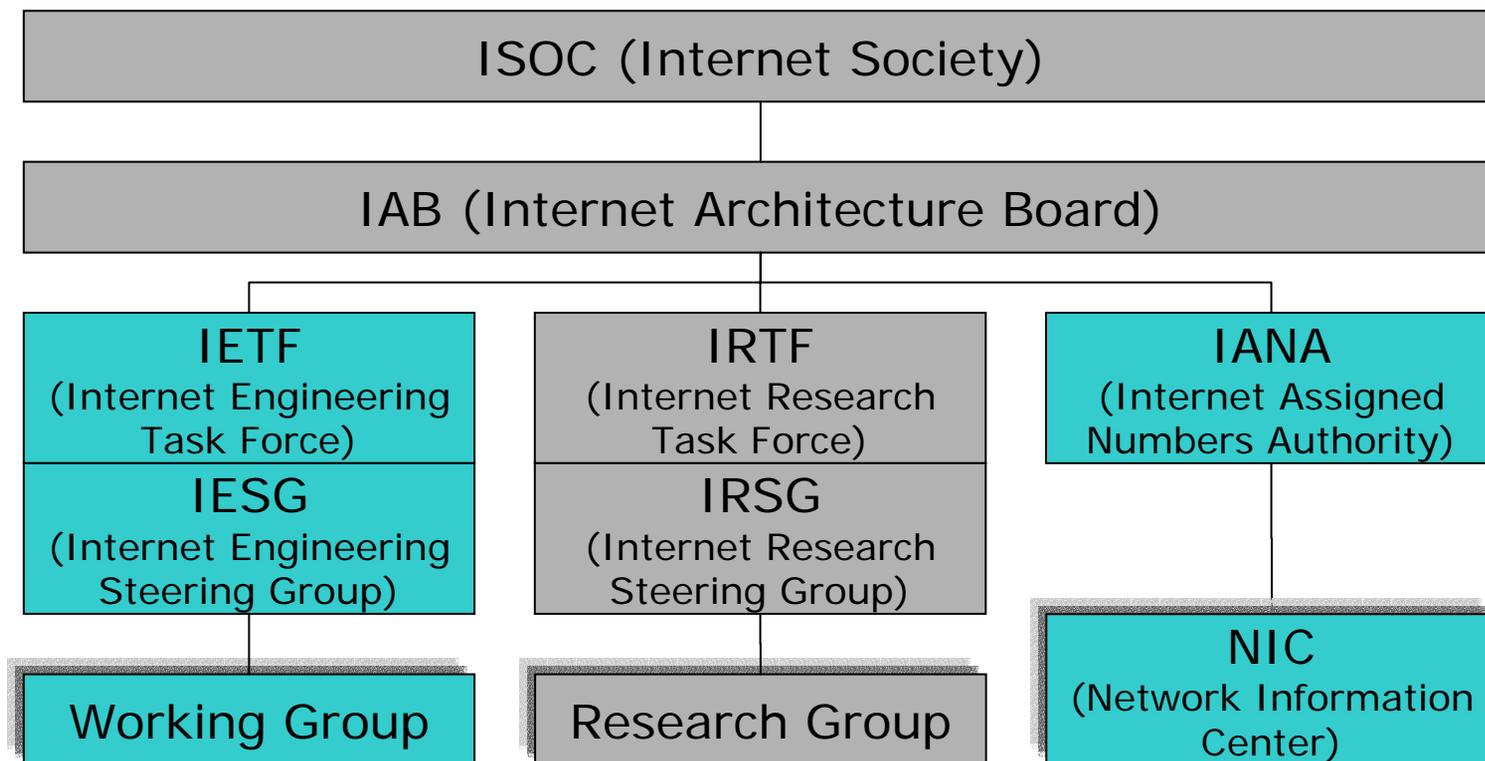
- IPv6のこれまで
 - 誕生の歴史
 - 基本的仕様と機能
 - 拡張的仕様と機能
- IPv6のこれから
 - 関連する新しい仕様
 - ユビキタス・ネットワークの話

提案の歴史

- 1991年7月
 - IPv6アドレスが不足するという研究報告に対するIETFの調査開始
- 1992年11月
 - RFC1380 “IESG Deliberations on Routing and Addressing”において調査結果報告
 - 次世代インターネットプロトコル検討開始
- 1993年12月
 - RFC1550 “IP: Next Generation (IPng) White Paper Solicitation”において要求条件提案
- 1995年1月
 - RFC1752 “The Recommendation for the IP Next Generation Protocol”においてIPv6へと改名
- 1995年12月
 - RFC1884 “IP Version 6 Addressing Architecture”において128bitアドレス空間の利用方法提案(現在は、RFC3513(2003))
- 1998年12月
 - RFC2430 “Internet Protocol, Version 6 (IPv6) Specification”などにおいて標準仕様決定

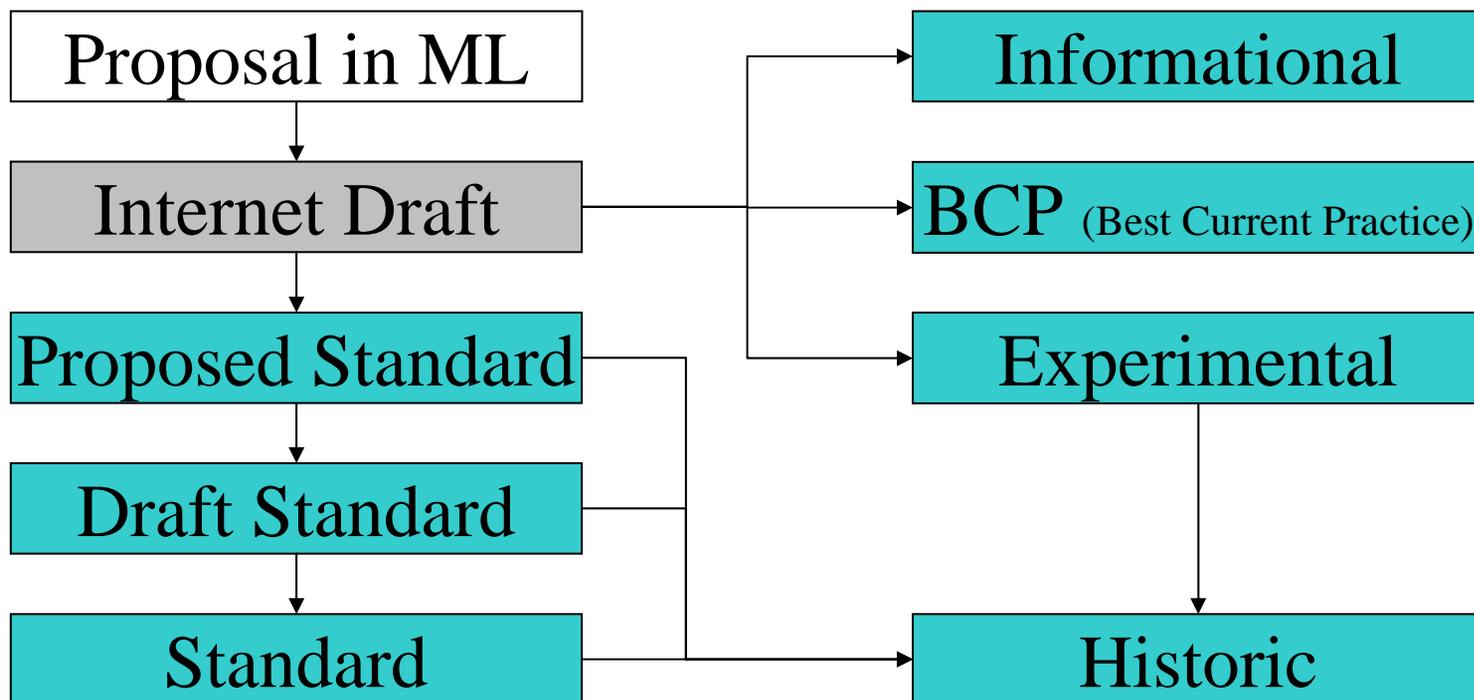
インターネットの標準化団体

○ Internet Societyの構造



インターネット標準ができるまで

○ IETFにおける標準(RFC)化のプロセス



IPngにおける選定基準(RFC1726)

1. 構造的に簡単であること
2. 複数の上位プロトコルをサポートすること
3. 長期に渡って適用できること
4. 発展的であること
5. 統制されない、分散協調指向であること

IETF における IPng 議論

- RFC1752における次世代プロトコル候補
 - CATNIP
 - ISO CLNPをベースにIP, IPX, OSIを統合する技術
 - SIPP
 - IPv4をベースにアドレス空間の64bit化などの改良技術
 - TUBA
 - ISO CLNPをベースに可変長アドレスを採用した技術
- SIPPのアドレスを128bitとしたものをベースに
IPv6が誕生

IPv6に関するWorking Group

- IPv6コア技術の議論
 - IPng (IP Next Generation) WG
 - 現在は、IPv6 WG
- IPv6利用技術の議論
 - ngtrans (Next Generation Transition) WG
 - 現在は、v6ops WG
- 拡張的新技术の議論
 - IPsec WG
 - mobileip WG
 - multi6 WG

本日の内容

- IPv6のこれまで
 - 誕生の歴史
 - **基本的仕様と機能**
 - 拡張的仕様と機能
- IPv6のこれから
 - 関連する新しい仕様
 - ユビキタス・ネットワークの話

IPv6の特徴

- たくさんのアドレス
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- プラグ&プレイによる簡単な設定
- IPv4からの単純で柔軟な移行
- セキュリティやモビリティ、リアルタイム性確保等の機能の標準実装

IPv6の特徴

- **たくさんのアドレス**
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- プラグ&プレイによる簡単な設定
- IPv4からの単純で柔軟な移行
- セキュリティやモビリティ、リアルタイム性確保等の機能の標準実装

たくさんのアドレス

- IPv6アドレス空間は128bit
 - IPv4アドレス空間の4倍
- IPv6アドレス数は 3.4×10^{38} 個
 - IPv4の 2^{96} 倍のアドレス数
- 例えば、
 - 地球上にばら撒くと 1cm^2 あたり 2.2×10^{20} 個
 - 人類全員で分けると1人あたり 4.9×10^{28} 個

アドレス空間比較 IPv4 vs. IPv6



IPv6アドレスの表記法 (RFC3513) その1

- 長いアドレスを示す簡潔な表記法
 - 16進数で表現する
 - 16bit毎に区切り文字”:” (コロン)を入れる
 - 例
 - FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
- ちなみに
 - IPv4と同様の表記法にすると、
 - 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255

IPv6アドレスの表記法 その2

○ 省略記法

- ブロック内の上位の”0”を省略できる

- [省略なし] 1080:0000:0000:0000:0008:0800:200C:0417
- [省略あり] 1080:0:0:0:8:800:200C:417

- 連続する”0”のブロックを”::”に省略できる

- [省略なし] 1080:0:0:0:8:800:200C:417
- [省略あり] 1080::8:800:200C:417A

- 但し、2箇所以上は省略できない

- [省略なし] 0:1080:0:0:8:800:200C:417
- [間違い] ::1080::8:800:200C:417A
- [省略あり] 0:1080::8:800:200C:417

or ::1080:8:800:200C:417

IPv6アドレスの表記法 その3

- ネットワーク・プレフィックスの表記法
 - IPv6アドレス"/"プレフィックス長という表記法
 - IPv6アドレスと同じ省略記法
 - 例
 - 12AB:0000:0000:CD30:0000:0000:0000:0000/60
 - 12AB::CD30:0:0:0:0/60
 - 12AB:0:0:CD30::/60
 - 誤
 - 12AB:0:0:CD3/60
 - 12AB::CD30/60
 - 12AB::CD3/60

IPv6アドレスの種類

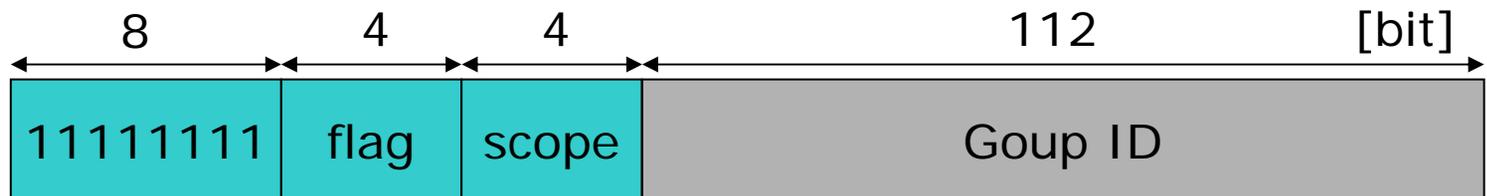
○ 上位ビットでIPv6アドレスの種類を指定



● 00...0 (::/128)	Unspecified
● 00...1 (::1/128)	ループバック
● 11111111 (FF00::/8)	マルチキャスト
● 1111111010 (FE80::/10)	リンクローカルユニキャスト
● <u>1111111011 (FEC0::/10)</u>	<u>サイトローカルユニキャスト</u>
● それ以外	グローバルユニキャスト

マルチキャストアドレス

- インタフェースの集合を表すアドレス
- 各インタフェースは複数のマルチキャストグループに属することができる



flag: 永続的 or 一時利用フラグ

scope: マルチキャストグループの範囲

- アドレス表記例

- FF02::1

リンクローカル・ユニキャストアドレス

- 自動アドレス設定や近隣探索において使用
- 単一のリンクのみにおいて有効で、ルータが存在しないネットワークでも利用可能



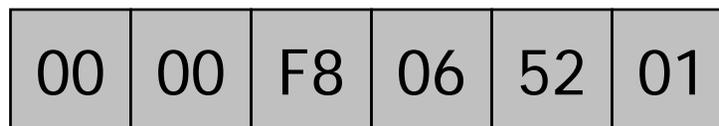
○ アドレス表記例

- FE80::200:F8FF:FE06:5201

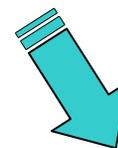
インタフェース識別子

- サブネットプレフィックス中で一意のアドレス
- 48bit MACアドレスよりID (EUI-64アドレス) を生成できる
- EthernetでのEUI-64アドレス生成例

MACアドレス
(48bit)



Universal/Local bit反転



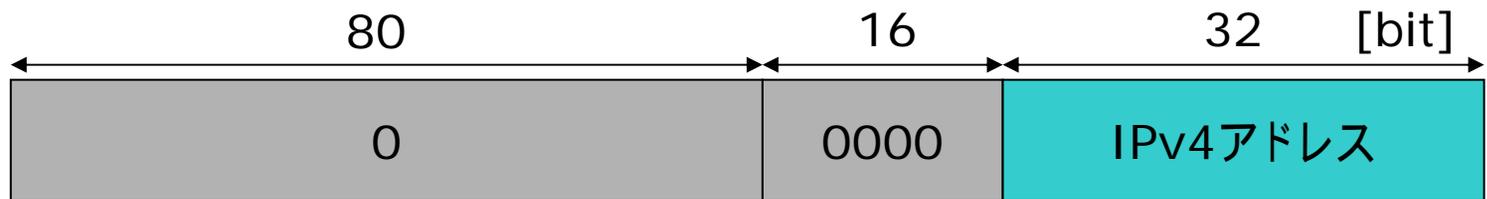
FFFE挿入

EUI-64アドレス
(64bit)

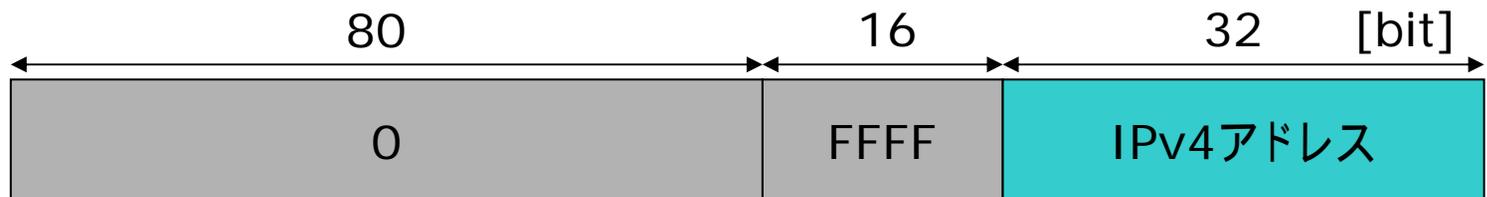


IPv4が埋め込まれたIPv6アドレス

- IPv6機器がIPv4機器と通信する際に使用
- IPv4互換IPv6アドレス



- IPv4射影IPv6アドレス



- アドレス表記例

- `::FFFF:129.144.52.38`

IPv6の特徴

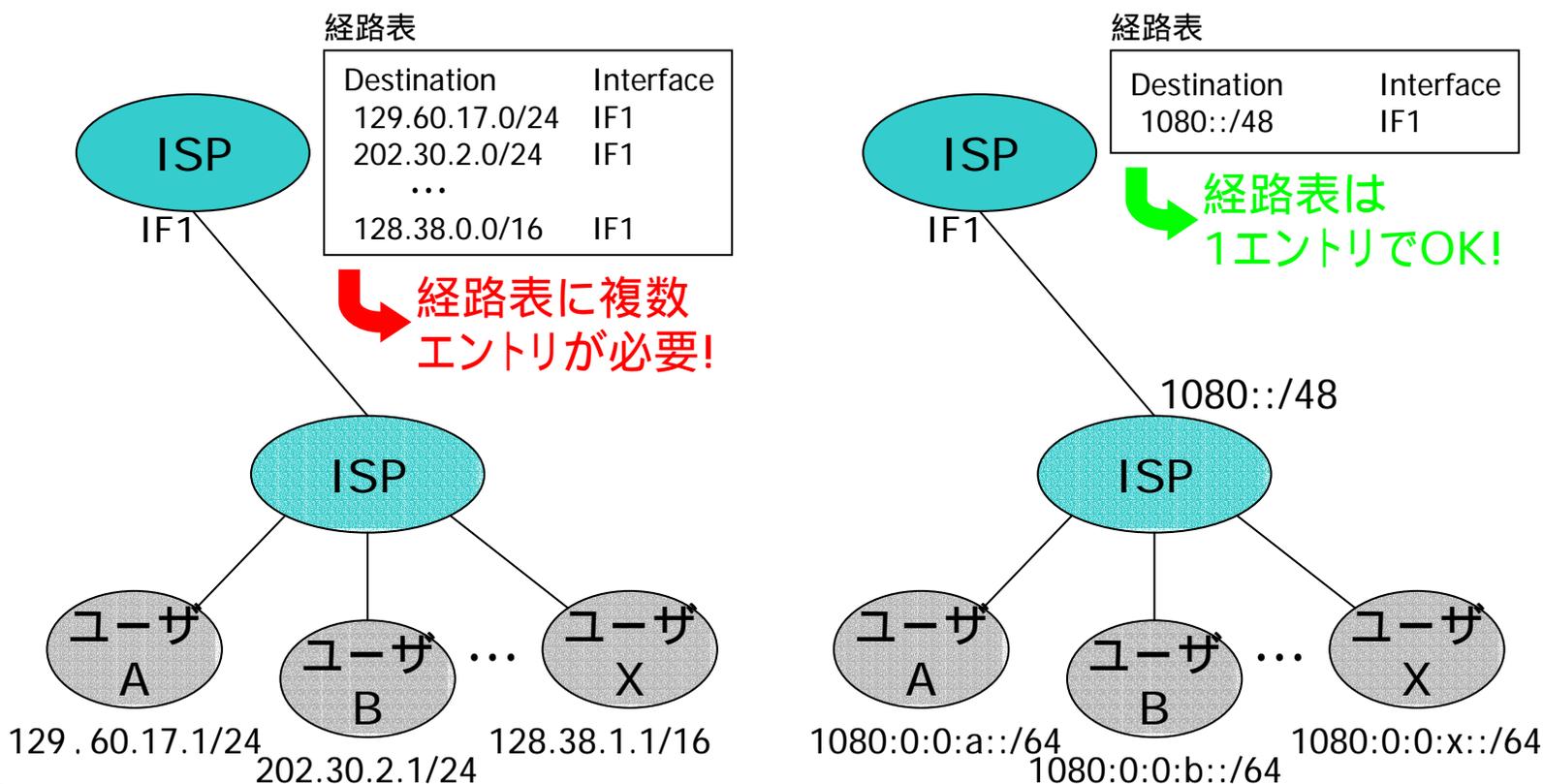
- たくさんのアドレス
- **集約できる経路情報**
- 単純なヘッダ構成、細分化の防止
- プラグ&プレイによる簡単な設定
- IPv4からの単純で柔軟な移行
- セキュリティやモビリティ、リアルタイム性確保等の機能の標準実装

集約できる経路情報

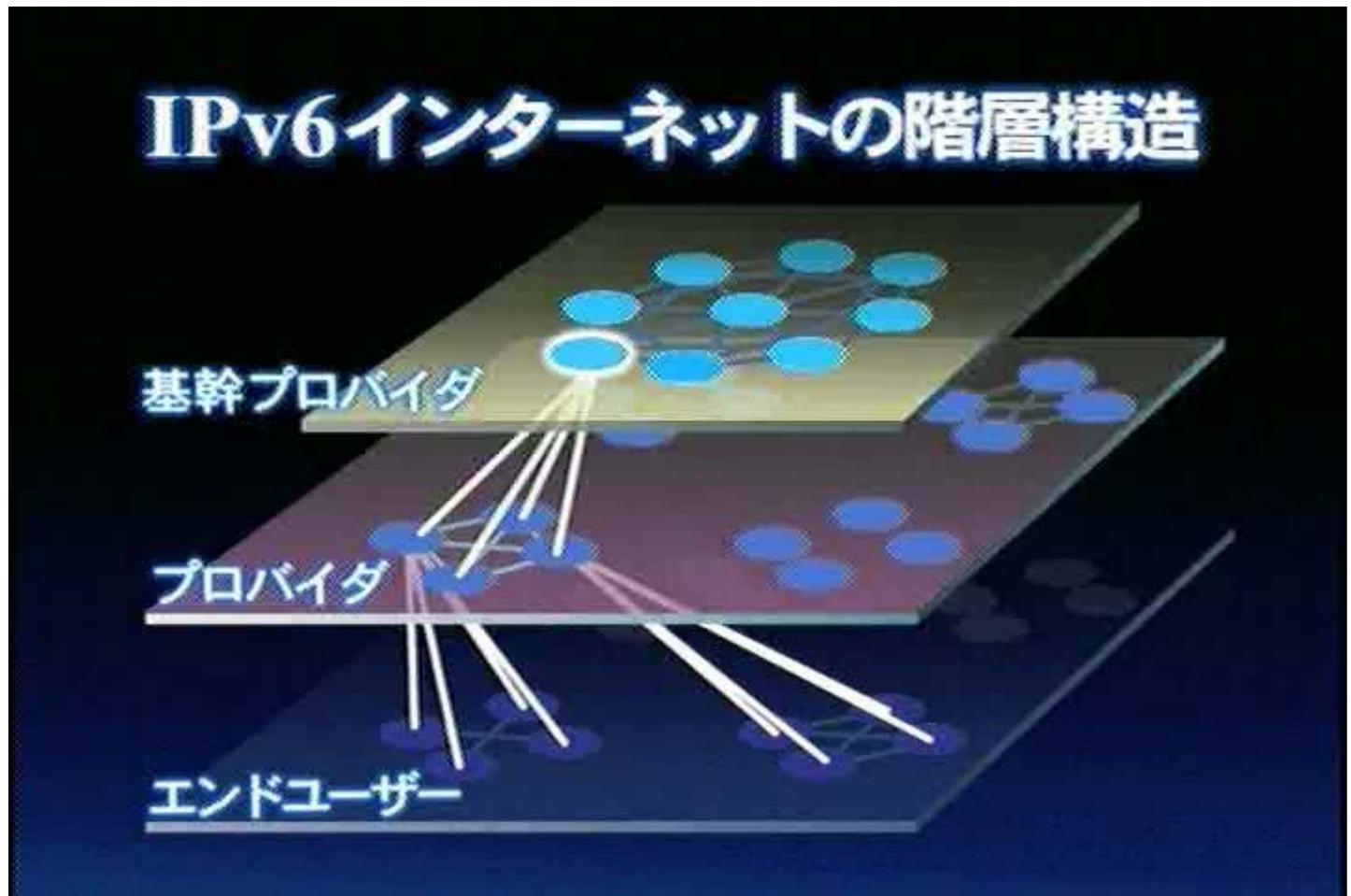
- 効率的に経路情報を集約できる構造
 - クラスレスなアドレス構造
 - ネットワーク構造に応じたアドレス割り振り
 - 同一ネットワークへの連続したアドレスブロック割り振り

経路集約の仕組み

○ 階層的ネットワーク構造による経路集約

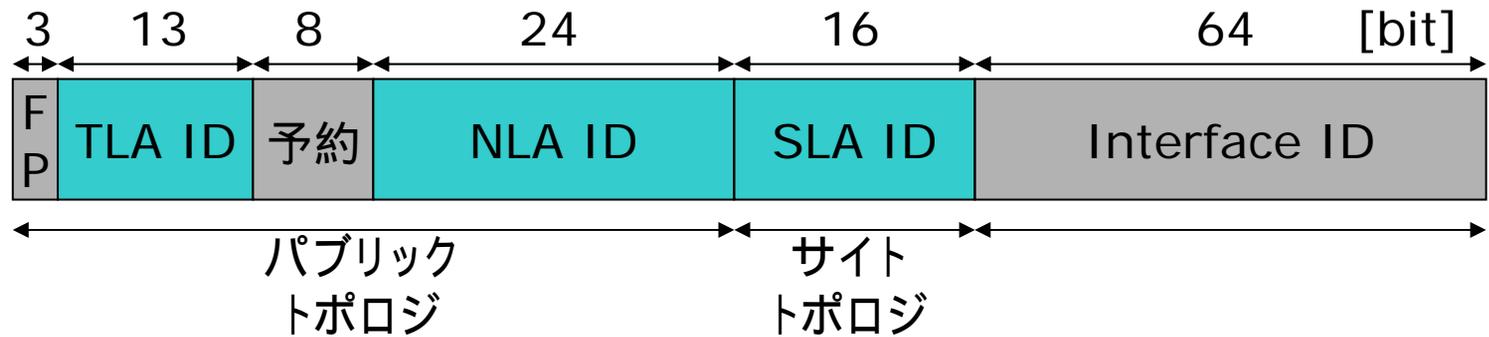


IPv6インターネットの一般的構造



【旧】グローバルアドレス形式 (RFC2374)

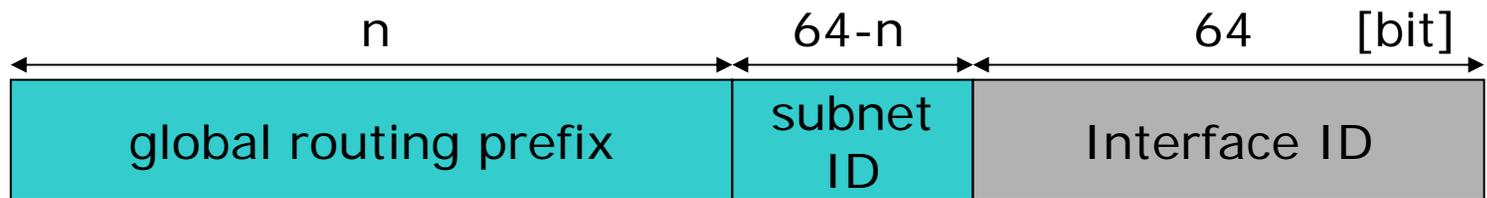
○ ネットワークトポロジに応じた階層構造



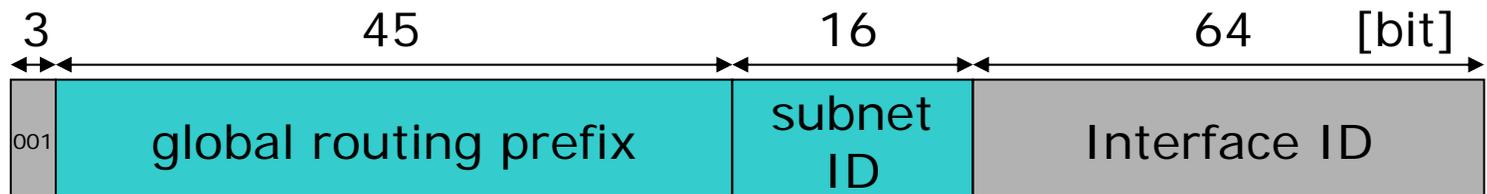
- FP アドレス形式プレフィックス (001)
- TLA ID 最上位階層集約子
- NLA ID 次階層集約子
- SLA ID サイト階層集約子
- Interface ID インターフェース識別子

【新】グローバルアドレス形式 (RFC3587)

- 様々なネットワークトポロジに対応可能な柔軟な階層構造



- 現在IANAが割り振っているアドレス形式例



IPv6の特徴

- たくさんのアドレス
- 集約できる経路情報
- **単純なヘッダ構成、細分化の防止**
- プラグ&プレイによる簡単な設定
- IPv4からの単純で柔軟な移行
- セキュリティやモビリティ、リアルタイム性確保等の機能の標準実装

単純なヘッダ構成、細分化の防止

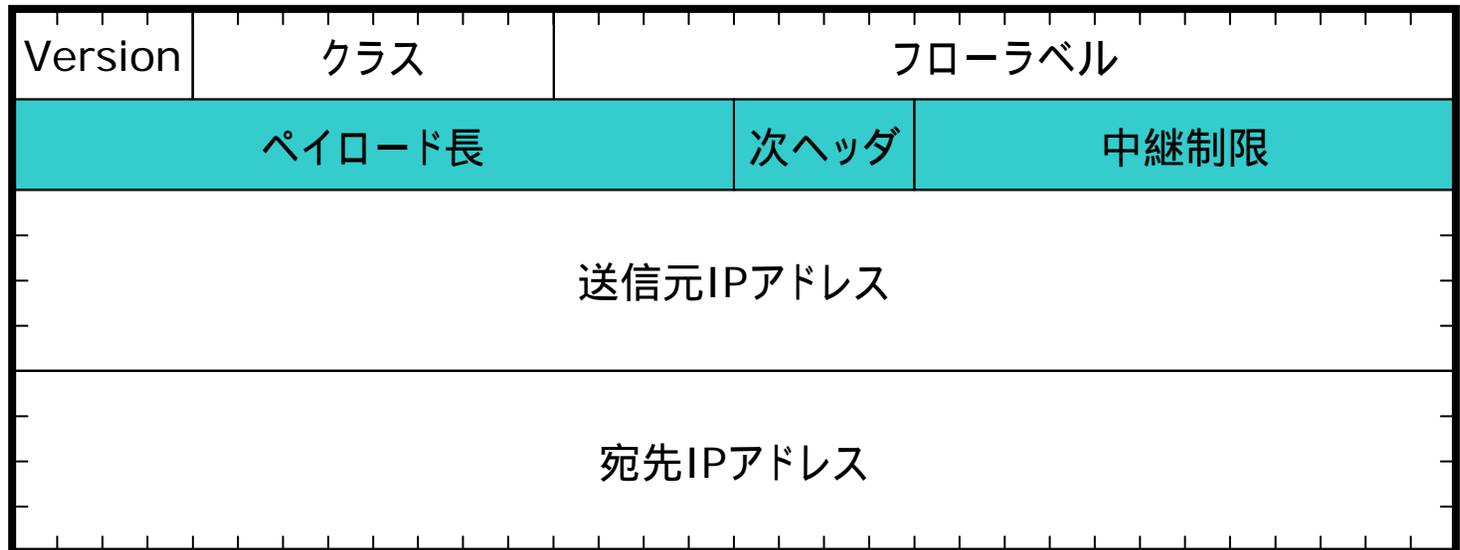
- IPv4の反省に基づく変更
 - 良い特徴はすべて継承
 - 不要な機能はすべて削除
 - 単純化による効率の向上
 - 将来の拡張性への配慮

IPv4 ヘッダフォーマット

Version	IHL	TOS	データグラム長	
ID		フラグ	オフセット	
TTL	プロトコル		ヘッダチェックサム	
送信元IPアドレス				
宛先IPアドレス				
オプション				パディング

- 利用すべきでないとは判断されたオプション
 - IHL: ヘッダ長が可変になると処理が複雑になる
 - TOS: 使われていない
 - ID, フラグ, オフセット: 細分化がある
 - プロトコル: 上位プロトコルは知らなくても良い
 - ヘッダチェックサム: 必要がない

IPv6 ヘッダフォーマット (RFC2460)



○ 新しく追加されたオプション

- クラス, フローラベル: 優先度の設定
- ペイロード長: 基本ヘッダより後ろの長さ
- 次ヘッダ: オプションヘッダが続く場合の種類
- 中継制限: データグラムの最大中継数

IPv6 ヘッダの IPv4 ヘッダとの違い

- アドレス空間の拡大
 - 32ビットから128ビットへ
 - 構造化アドレスの利用が可能
- 経路上のルータでの処理軽減
 - ヘッダ構造の簡素化
 - 固定長ヘッダ
 - ヘッダチェックサム廃止
- 高い拡張性
 - 拡張ヘッダによるオプション形式の利用

経路中での細分化禁止

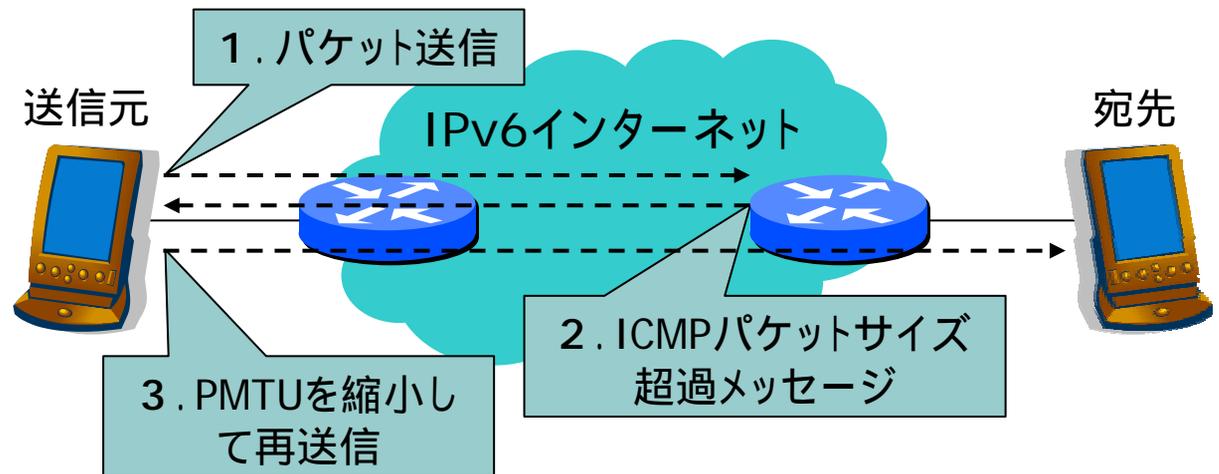
- ルータ負荷の原因である細分化禁止
 - 経路途中で細分化を起こさないために、
 - ネットワークにはリンク毎に異なるMTUが存在
 - MTU: Maximum Transfer Unit
 - MTU以上のIPデータグラムを送ってはいけない
- 通信経路上の全てのリンクのMTUを調べ、その最小値にデータグラムサイズを設定

経路上の最小MTUを探索する機能が必要

経路上のMTU探索プロトコル

○ 動作

1. PMTU = 次の中継点のMTU(イーサネットの場合1500バイト)としてパケットを送信
2. 途中のルータからICMPパケットサイズ超過メッセージが送付
3. PMTUを縮小、送信元でフラグメント処理を行いパケットを送信(フラグメントオプションヘッダ使用)



IPv6の特徴

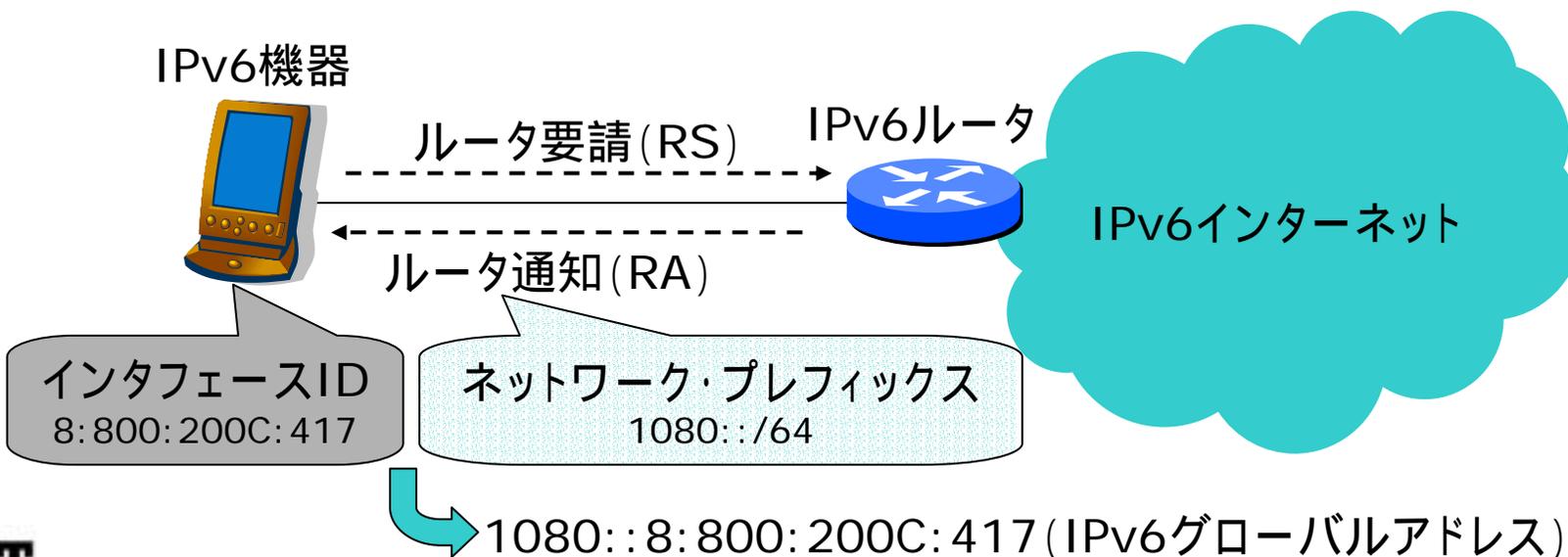
- たくさんのアドレス
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- **プラグ&プレイによる簡単な設定**
- IPv4からの単純で柔軟な移行
- セキュリティやモビリティ、リアルタイム性確保等の機能の標準実装

プラグ&プレイによる簡単な設定

- **アドレス自動設定** (Address Autoconfiguration)
 - **ネットワーク設定作業の軽減**
 - ステートレス・アドレス自動設定
 - ステートフル・アドレス自動設定(DHCPv6)
- **近隣探索プロトコル** (Neighbor Discovery)
 - IPアドレス自動設定
 - データリンク層アドレスの解決
 - 近隣ルータの探索などに用いられる

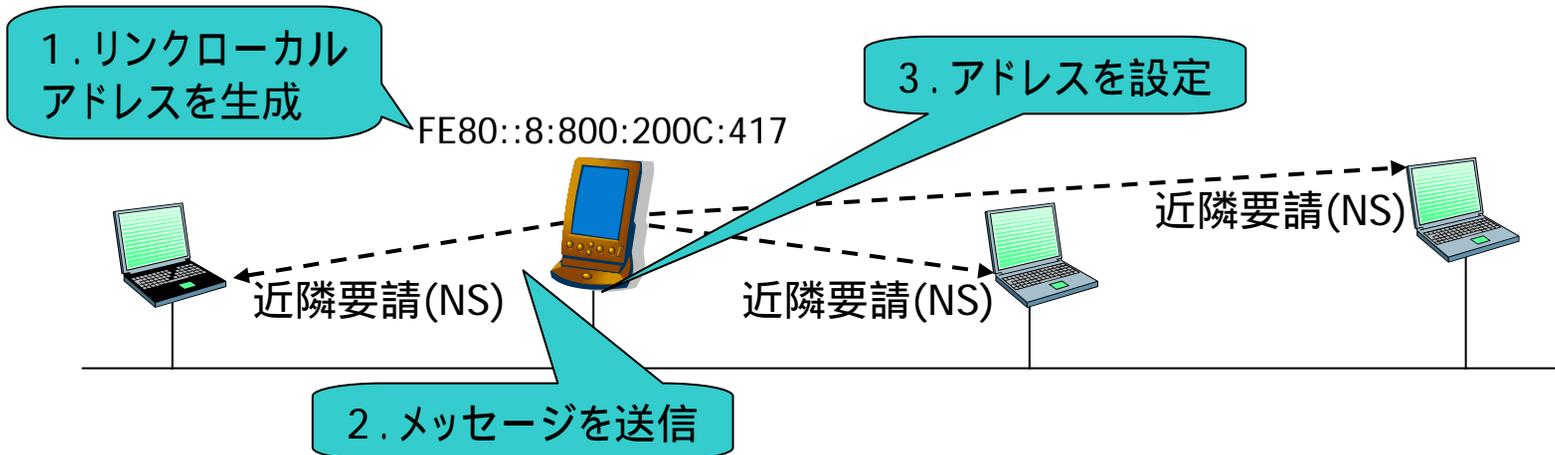
ステートレス・アドレス自動設定 (RFC2462)

- ルータから通知される情報
 - ネットワーク・プレフィックス
- IPv6機器自身が決定できる情報
 - インタフェースID
- この2つを組み合わせると IPv6 アドレスを生成



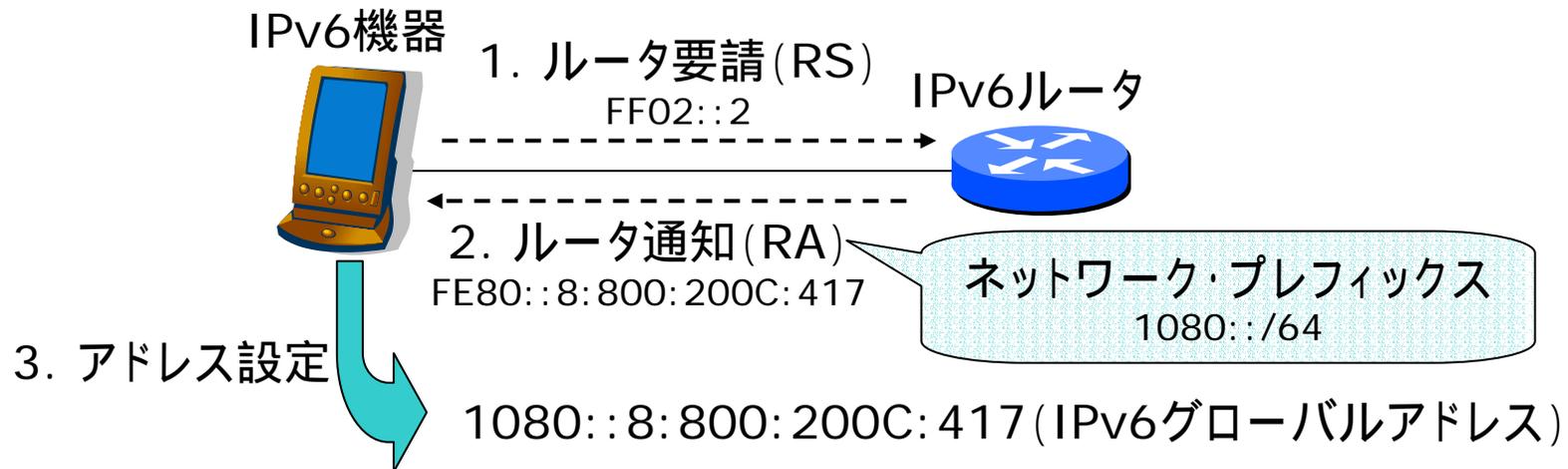
ステートレス・アドレス自動設定動作1

- フェーズ1 リンクローカル・ユニキャストアドレスの割り当て
 1. リンクローカル・ユニキャストアドレスの生成
 2. 生成したアドレスの唯一性を確認するため、近隣要請メッセージを送信
 3. 応答がなければインタフェースにアドレスを割り当てる



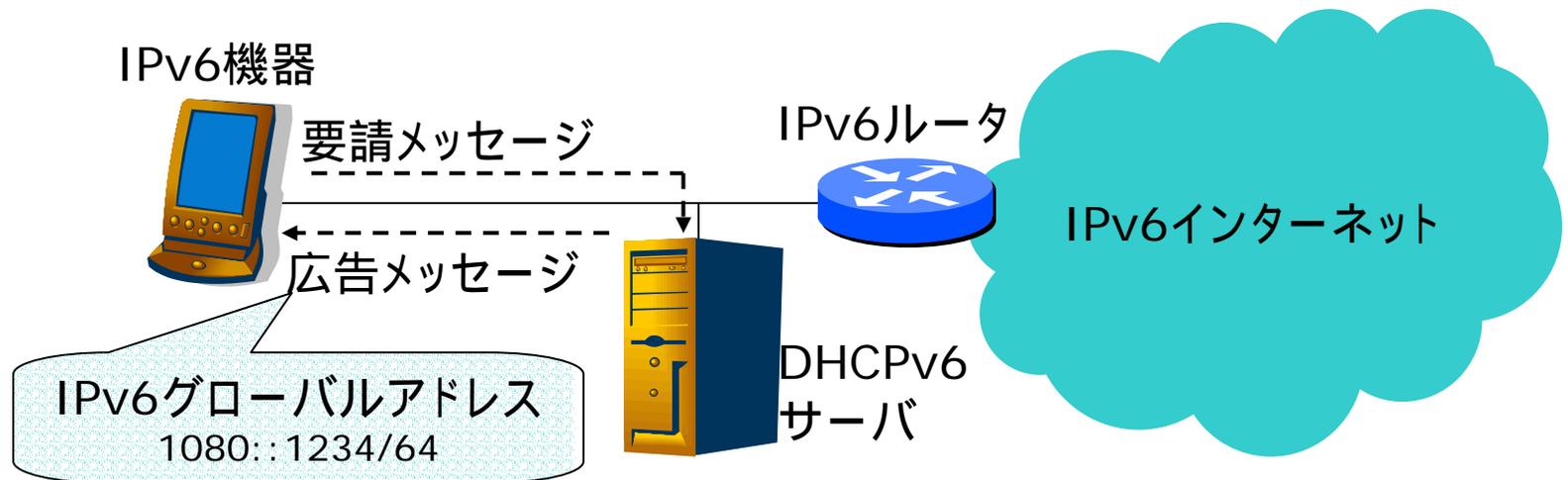
ステートレス・アドレス自動設定動作2

- フェーズ2 ルータ通知メッセージ処理
 1. ルータ通知メッセージを待つか、ルータマルチキャストグループにルータ要請メッセージを送信
 2. ルータは要請メッセージを受け取ったら、ルータ通知メッセージを送信
 3. ルータから送られたプレフィックスとインターフェイスIDよりアドレスを自動設定



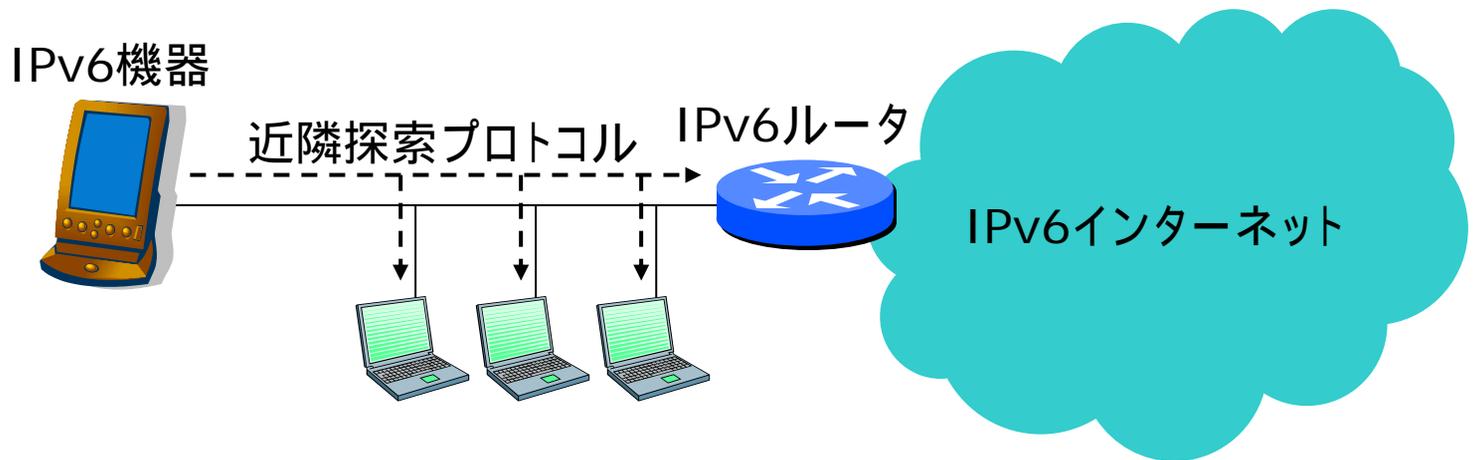
ステートフル・アドレス自動設定 (RFC3315: DHCPv6)

- サーバから通知される情報
 - IPv6アドレス(IPv4 DHCPと同様)
- ステートレス・アドレス自動設定との連携も可能
 - DNSサーバ情報などの通知



近隣探索プロトコル(RFC2461)

- データリンク層アドレスの解決
- 近隣ルータの探索
- IPv4 での ARP の役割を担う



近隣探索プロトコルの種類

- ルータ要請メッセージ (Router Solicitation Message)
- ルータ通知メッセージ (Router Advertisement Message)
 - アドレス自動設定や移動の検知等
 - アドレスプレフィックスを送付
- 近隣要請メッセージ (Neighbor Solicitation Messages)
- 近隣通知メッセージ (Neighbor Advertisement Message)
 - IPv4のARPと同等
- リダイレクトメッセージ (Redirect Message)
 - IPv4のICMPリダイレクションと同等

IPv6の特徴

- たくさんのアドレス
- 集約できる経路情報
- 単純なヘッダ構成、細分化の防止
- プラグ&プレイによる簡単な設定
- **IPv4からの単純で柔軟な移行**
- セキュリティやモビリティ、リアルタイム性確保等の機能の標準実装

IPv4からの単純で柔軟な移行

- IPv4からIPv6への変更に際して、
 - 移行を行うために必要なことは何か？
 - IPのプロトコル変更により必要となるサービスのな変更は何か？
 - どのタイミングでどのように移行すればよいか？
 - IPv4は使えなくなってしまうのか？

移行による影響

	ホスト	ルータ
アプリケーション層 (HTTP, SMTP, RTP)	アプリケーション	ルータ制御 アプリケーション
トランスポート層 (TCP, UDP)	オペレーティング システム	ルータ制御OS
インターネット層 (IP)		経路制御部
ネットワーク層 (Ethernet, ATM)	ドライバ	ドライバ

移行による影響

	ホスト	ルータ
アプリケーション層 (HTTP, SMTP, RTP)	アプリケーション 一部要変更	ルータ制御 アプリケーション 一部要変更
トランスポート層 (TCP, UDP)	オペレーティング システム 要変更	ルータ制御OS 要変更
インターネット層 (IP)		経路制御部 要変更
ネットワーク層 (Ethernet, ATM)	要変更	要変更

- IPを用いる全ての部分に変更が必要

変更が必要となるノード機能

- アプリケーション
 - IPv6アドレス表記の入出力(GUIなど)
 - TCP/IPとのアプリケーションインタフェース部分
- オペレーティングシステム
 - IPv6アドレス表記の解釈
 - IPv6固有機能の実装
 - インタフェースデバイスドライバのIPv6対応
 - IPv6経路情報の管理

ネットワークサービスのIPv6対応状況

○ 基本サービス

- Windows Media Technologiesなど商用ソフトウェアが対応開始
- DNS、HTTP、SMTP、POPなど基本サービスのオープンソース・ソフトウェアはほぼ対応済

○ 開発ツール

- Visual Studio、Borland(R) Enterprise Server、Wind River Platform、ソフトフロント SPPなど商用開発ツールが対応開始
- J2SE、GCCなどオープンソース開発ツールは従来より対応済

IPv6対応ネットワークサービス製品

- Radius
 - アクセンス・テクノロジー: fullflex MG
 - ステラクラフト: Enterpas Pro 4.1
- プロキシ/キャッシュサーバ
 - ネットワークアプライアンス: NetCache 5.5
- SIP/SIMPLE
 - 日立: PROGNET
- 負荷分散スイッチ
 - F5ネットワークスジャパン: BIG-IP
- IPv6/IPv4変換
 - 富士通: IPCOM v4/v6 Translator
 - 横河電機: TTB

IPv6style(www.ipv6style.jp)より

IPv6対応ネットワークセキュリティ製品

- チェックポイント・ソフトウェア・テクノロジーズ
 - VPN-1/FireWall-1
- ノキア・ジャパン
 - ノキアIPセキュリティシリーズ
- ネットスクリーン
 - Netscreen
- インターネットセキュリティシステムズ
 - RealSecure, Proventiaシリーズ
- 日本HP
 - HP IceWall SSO 6.0
- 富士通LSIソリューションズ
 - IPsecアクセラレータLSI

IPv6style(www.ipv6style.jp)より

ネットワーク機器のIPv6対応状況(1)

○ ホスト

- Windows XP, Mac OS Xで対応済
- UNIX(Solaris, Linux, BSD etc.)は従来より対応済
- インターネット家電製品(AV機器、ゲーム機)の対応開始

○ ルータ

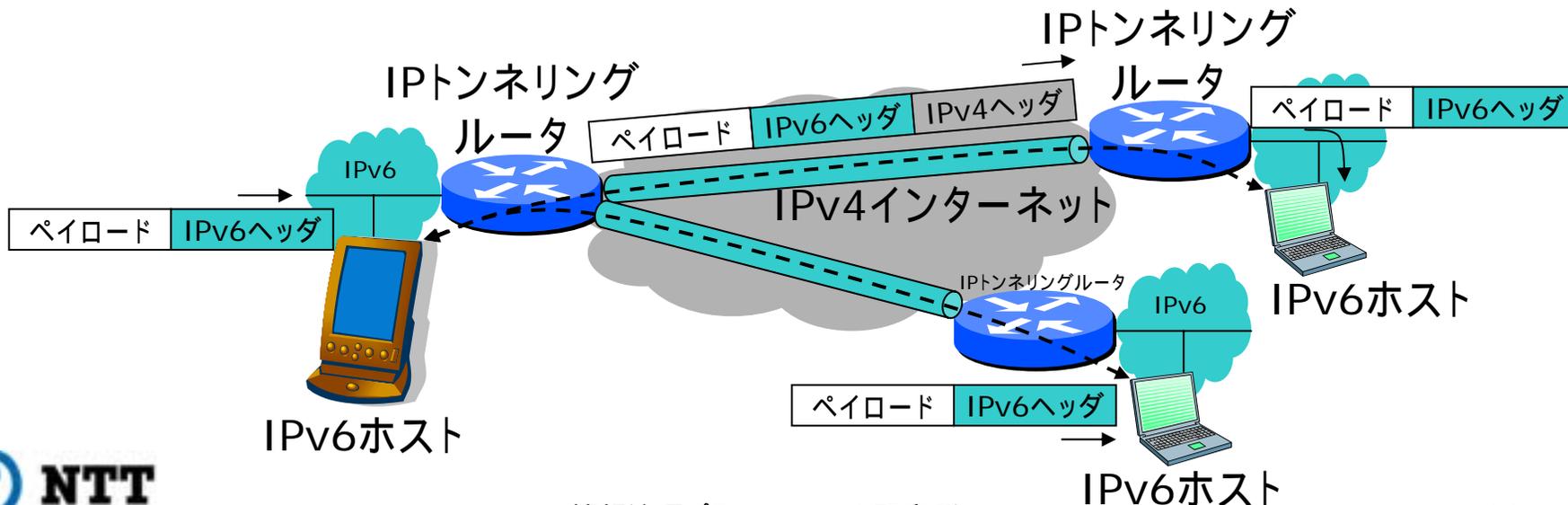
- 日立、NEC、富士通などの国内ベンダは、ハードウェア転送可能なIPv6ルータを出荷中
- Cisco, Juniper, Foundry, 6WIND, IP infusionなどの海外ベンダも対応済
- YAMAHA, Allied TelesisなどSOHOルータも対応済

移行へ向けたシナリオ

- 課題
 - IPv6ホストとIPv4ホストは直接通信不可能
 - あるタイミングでインターネット上の全てのネットワークをIPv6へ一斉に置き換えることは不可能
- 解決方針
 - スモールスタートから始めて、最終的に全てのネットワークをIPv6へ移行する
 - ネットワーク単位でルータを少しずつ置き換え移行を進める
 - ネットワークの中でもホストを少しずつ置き換え移行を進める
- 提案技術
 1. IPトンネリング
 2. デュアルIPスタック
 3. トランスレータ

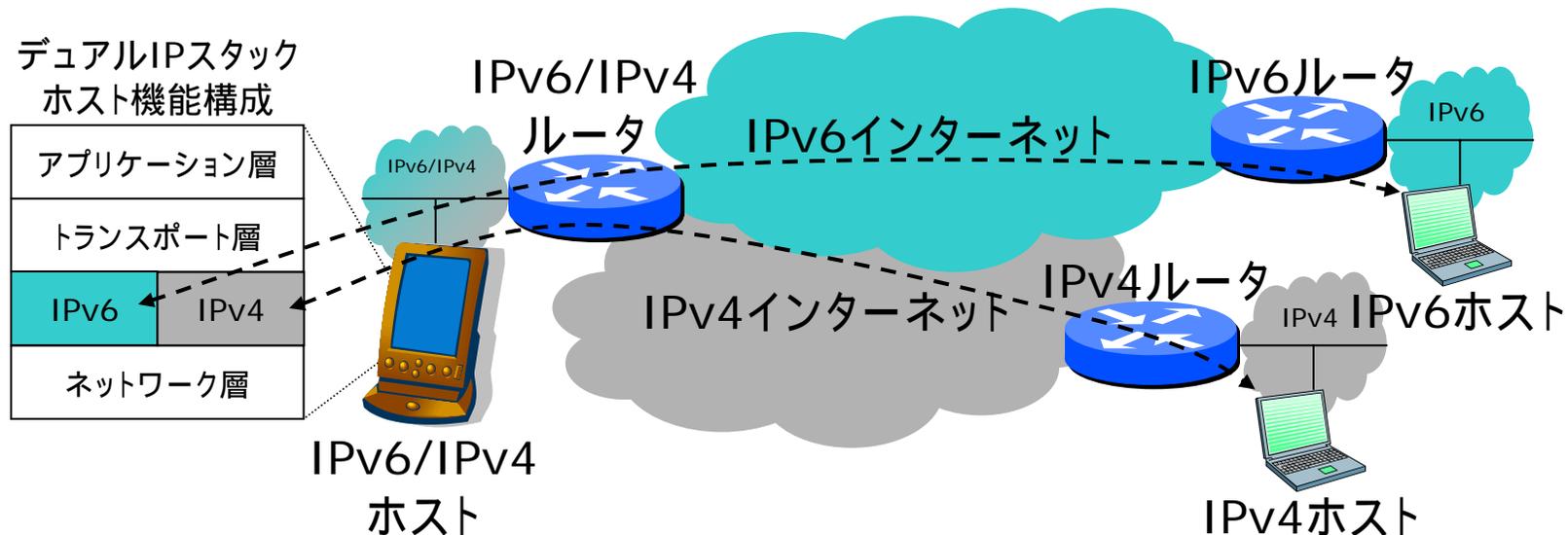
技術1: IPトンネリング

- 利用環境
 - 複数のIPv6ネットワークがIPv4ネットワークを介してつながっている
- 機能
 - IPv6パケットがIPv4ネットワークを通過することを可能にする
- 効果
 - 直接接続していないIPv6ネットワーク内のホストが通信可能になる



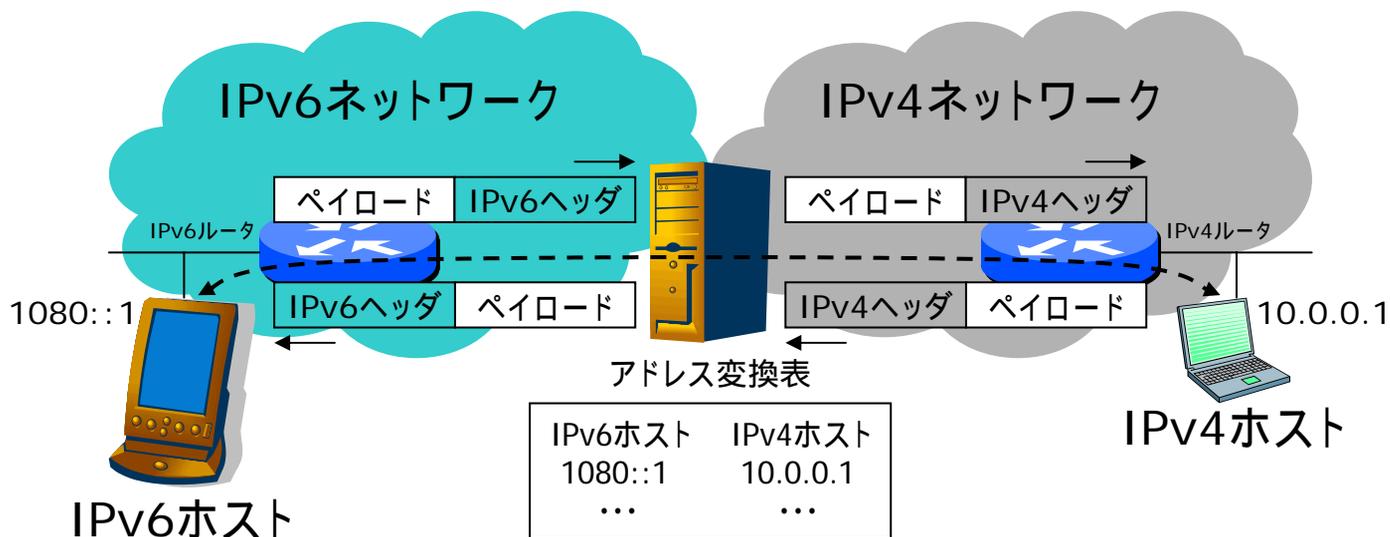
技術2: デュアルIPスタック

- 利用環境
 - IPv6とIPv4が共存するネットワーク
- 機能
 - ホストとルータがIPv6とIPv4の両通信機能を持つことを可能にする
- 効果
 - 1台のホストからIPv6とIPv4の両サービスへアクセス可能になる



技術3: トランスレータ

- 利用環境
 - IPv6ホストとIPv4ホストが共存するネットワーク
- 機能
 - IPv6ホストがIPv4ホストと通信することを可能にする
- 効果
 - IPv4ネットワーク上にしかないレガシーなサービスへIPv6からアクセス可能になる



IPv4/IPv6相互接続技術

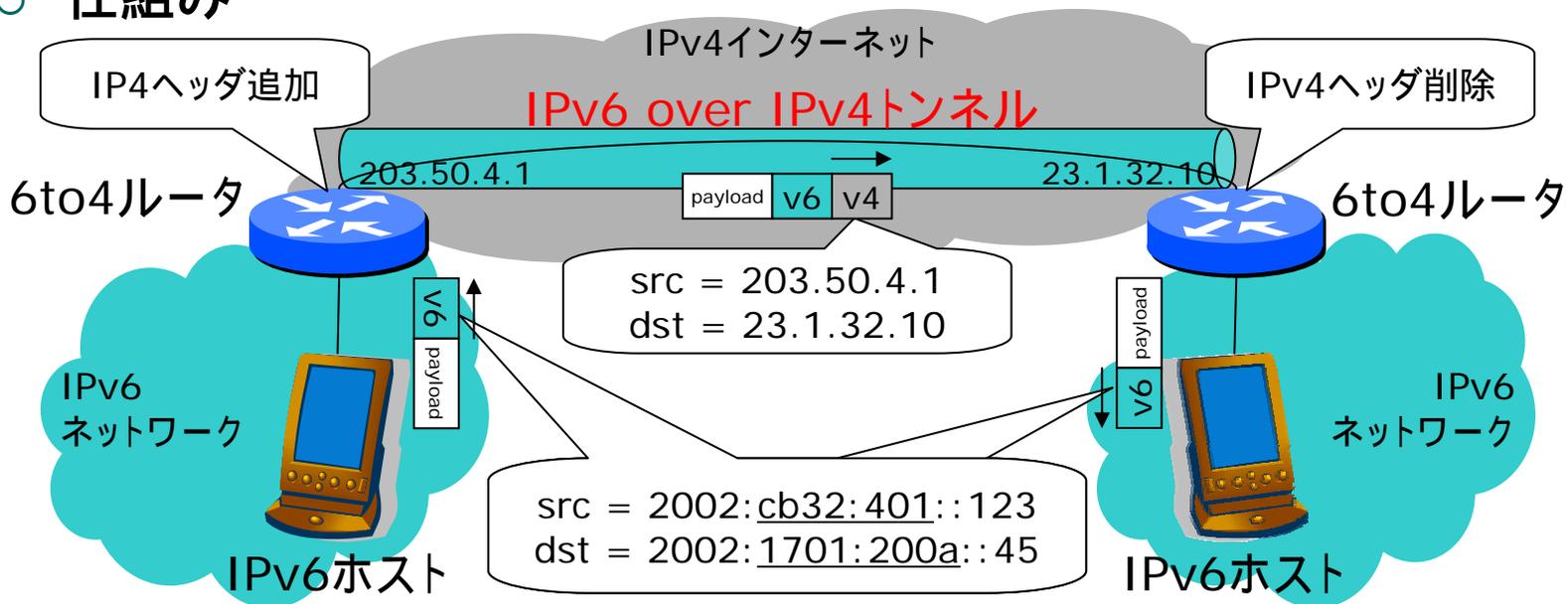
- トンネリング技術
 - 6to4
 - IPv6トンネルブローカー
 - ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)
 - DSTM (Dual Stack Transition Mechanism)
- デュアルスタック技術
 - BIS (Bump-In-the-Stack)、BIA (Bump-In-the-Application)
 - ホスト内でIPv4/IPv6変換を行い、IPv4アプリをIPv6ネットワークに対応させる
- トランスレータ技術
 - SIIT (Stateless IP/ICMP Translation Algorithm)
 - NAT-PT (Network Address Translation-Protocol Translation)
 - SOCKSベースIPv6/IPv4ゲートウェイ

トンネリング技術1: 6to4

○ 概要

- グローバルユニークなIPv4アドレスを埋め込んだIPv6アドレス (6to4アドレス) により、自動的にIPv6 over IPv4トンネルを生成する

○ 仕組み

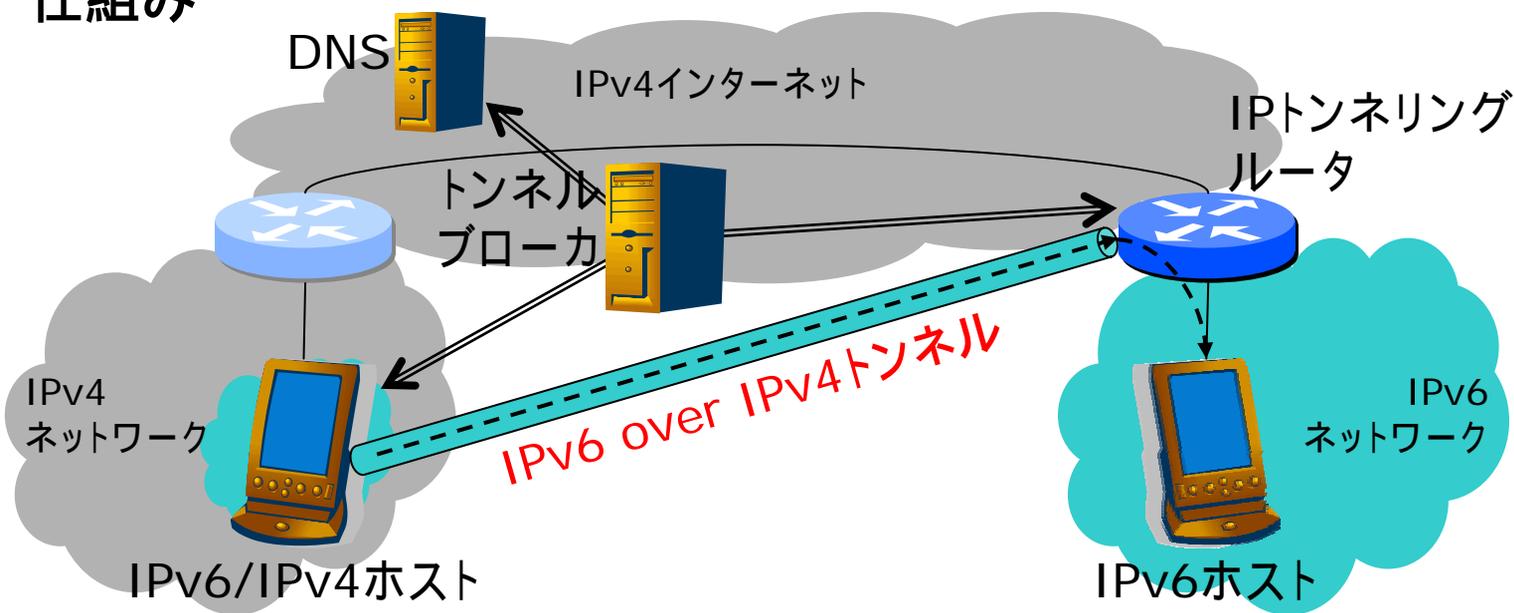


トンネリング技術2: IPv6トンネルブローカー

○ 概要

- トンネルを生成するための制御情報を管理するトンネルブローカーにより、端末とトンネル・サーバ間で自動的にIPv6 over IPv4トンネルを生成する

○ 仕組み

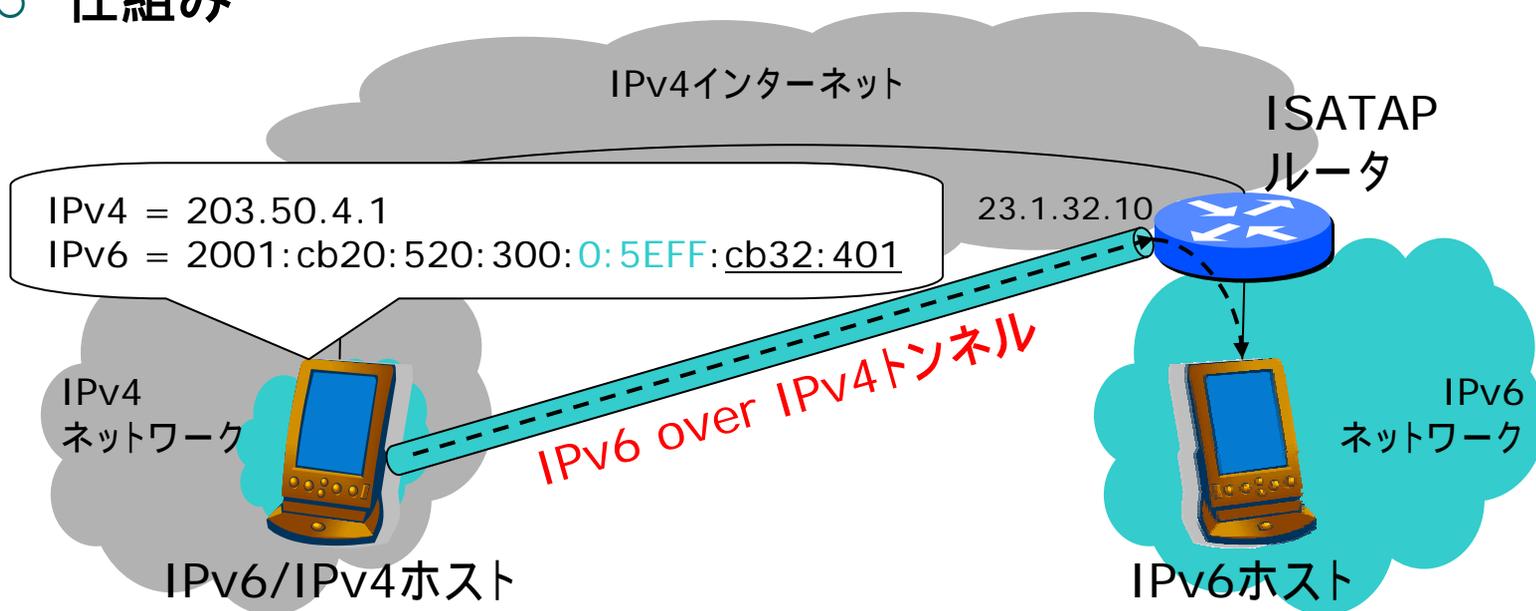


トンネリング技術3: ISATAP

○ 概要

- EUI-64フォーマットを活用して、サイトユニークなIPv4アドレスを埋め込んだIPv6アドレス (ISATAPアドレス) を利用し、自動的にIPv6 over IPv4トンネルを生成する

○ 仕組み

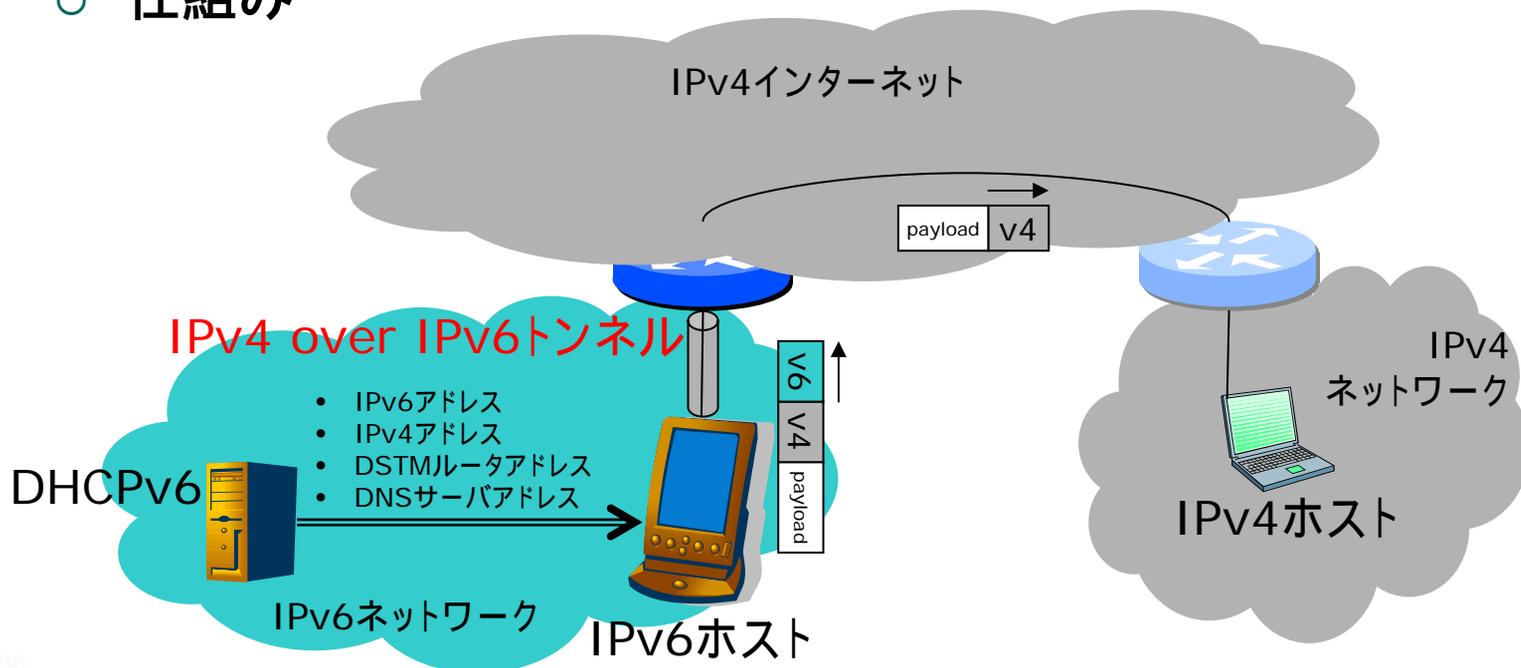


トンネリング技術4: DSTM

○ 概要

- DHCPv6を利用しIPv6ネットワーク中にIPv4 over IPv6トンネルを生成する

○ 仕組み

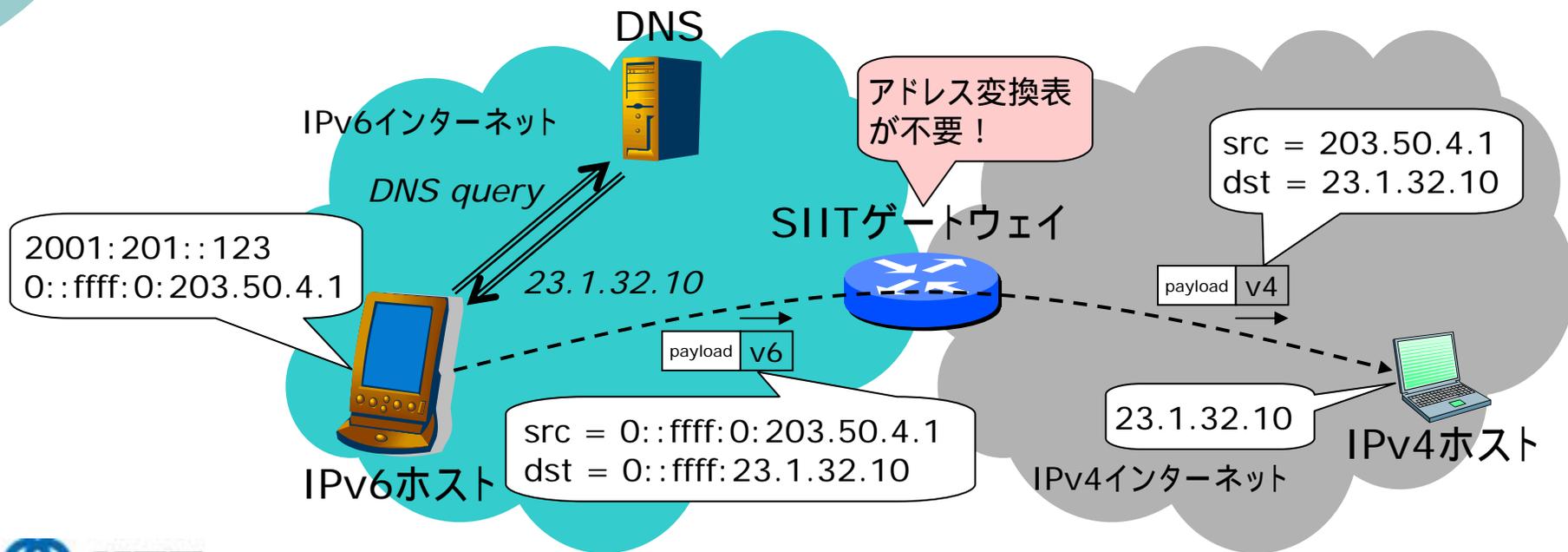


トランスレータ技術1: SIIT

○ 概要

- IPv4-translatedアドレスとIPv4-mappedアドレスを利用して、SIITゲートウェイでIPv4/IPv6変換を行う

○ 仕組み

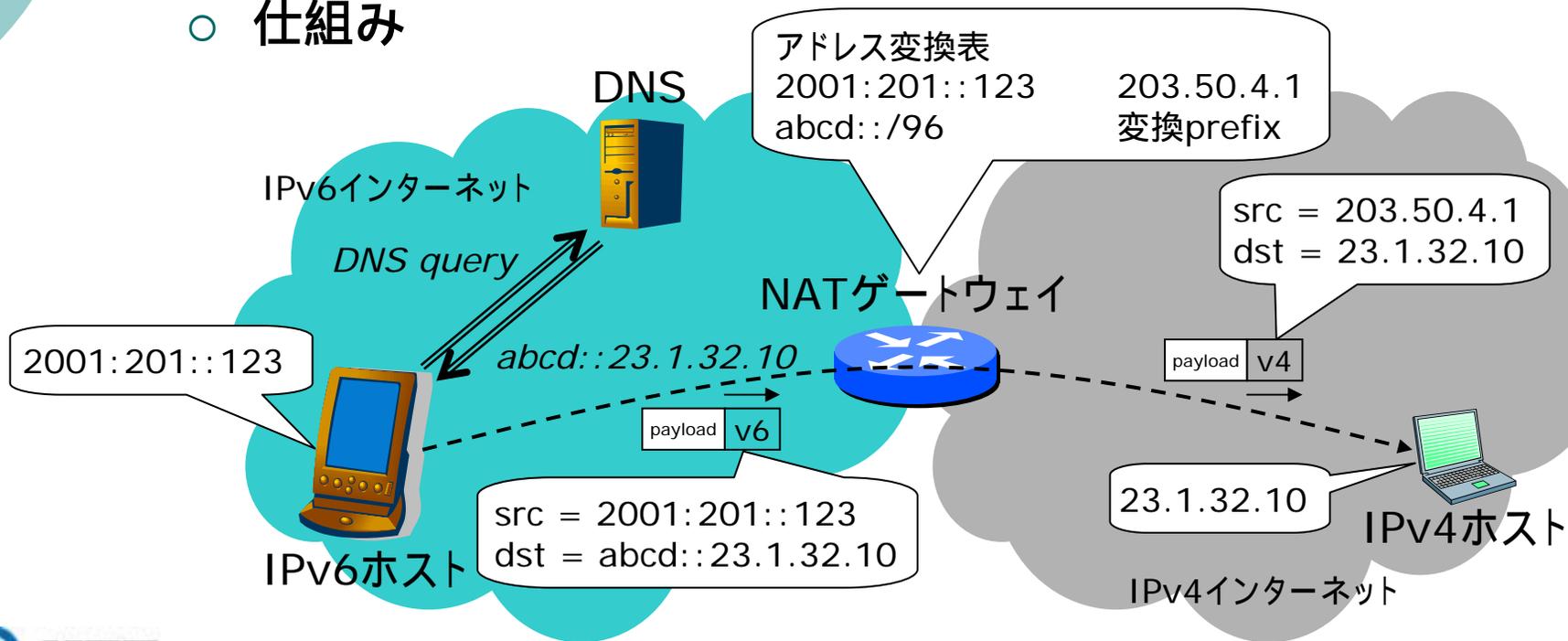


トランスレータ技術2: NAT-PT

○ 概要

- IPv6アドレスとIPv4アドレス&ポート変換テーブルを利用して NATゲートウェイでIPv4/IPv6変換を行う

○ 仕組み

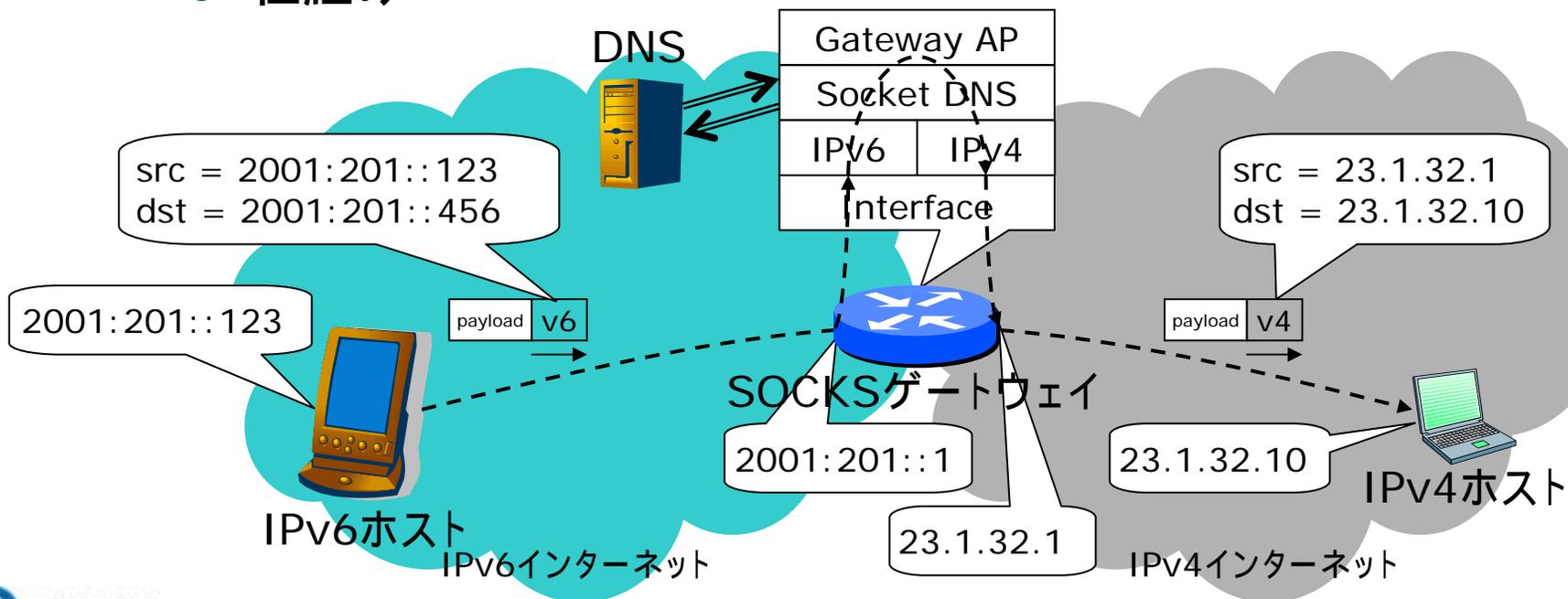


トランスレータ技術3: SOCKSベース IPv6/IPv4ゲートウェイ

○ 概要

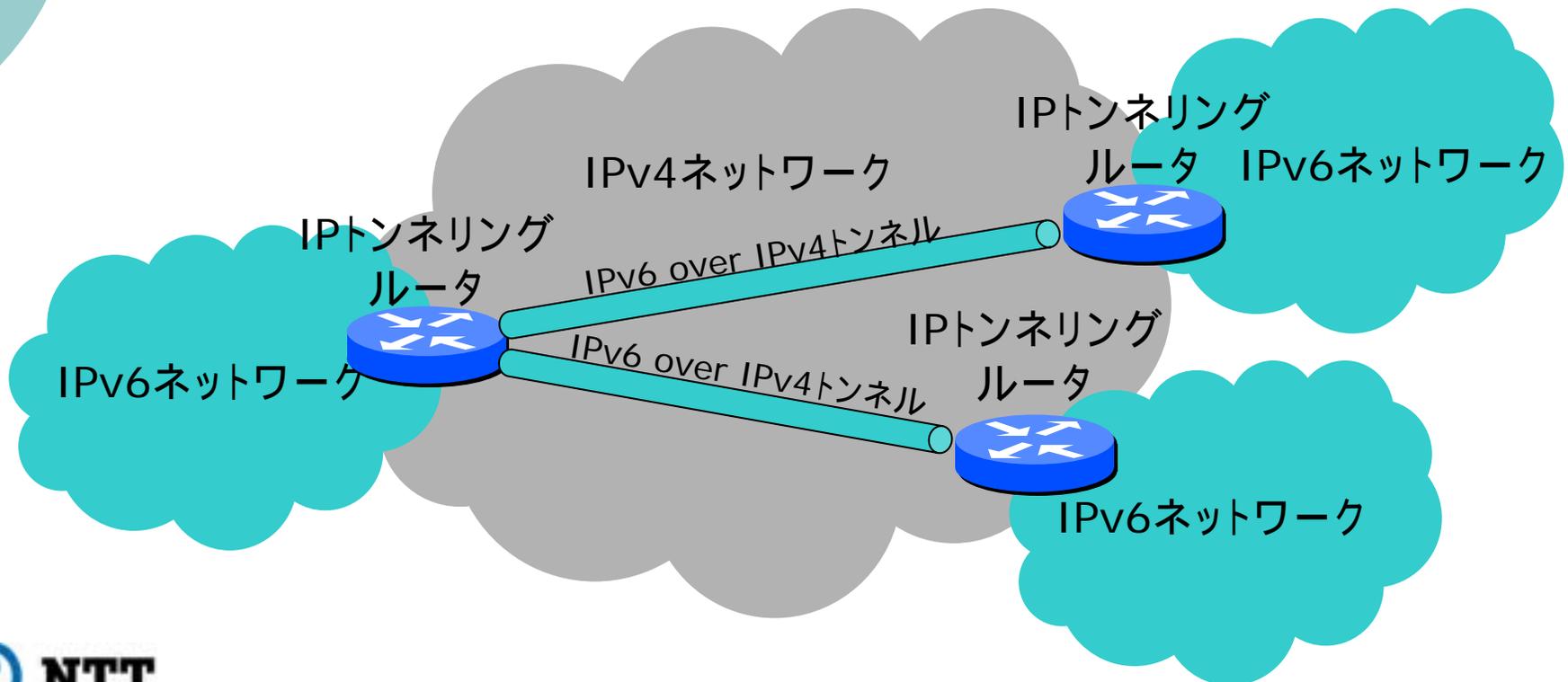
- IPv6アドレスのSocketとIPv4アドレスのSocketをproxyするSOCKSゲートウェイでIPv4/IPv6変換を行う

○ 仕組み



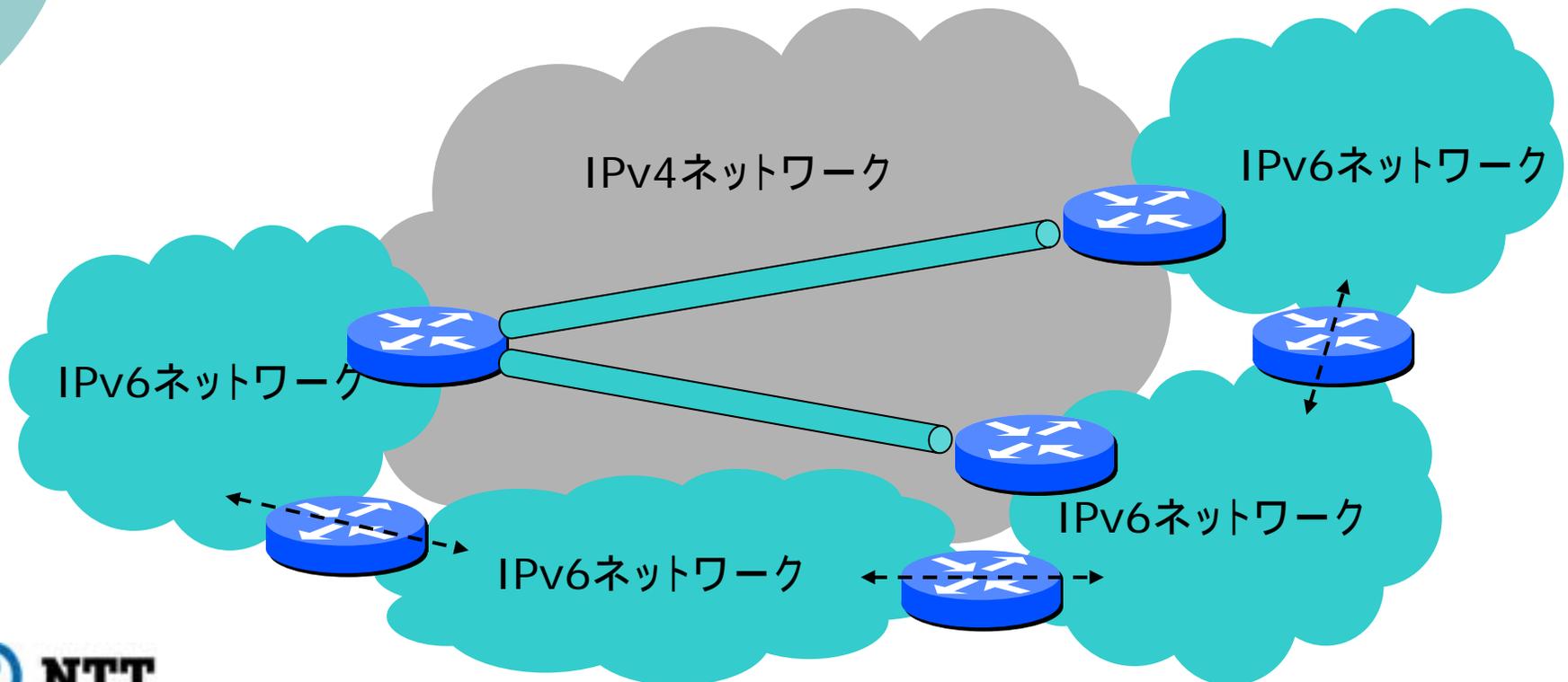
移行シナリオ (第1段階)

- IPv4ネットワーク >> IPv6ネットワークの時
 - IPv6 over IPv4トンネリングによるネットワーク構築



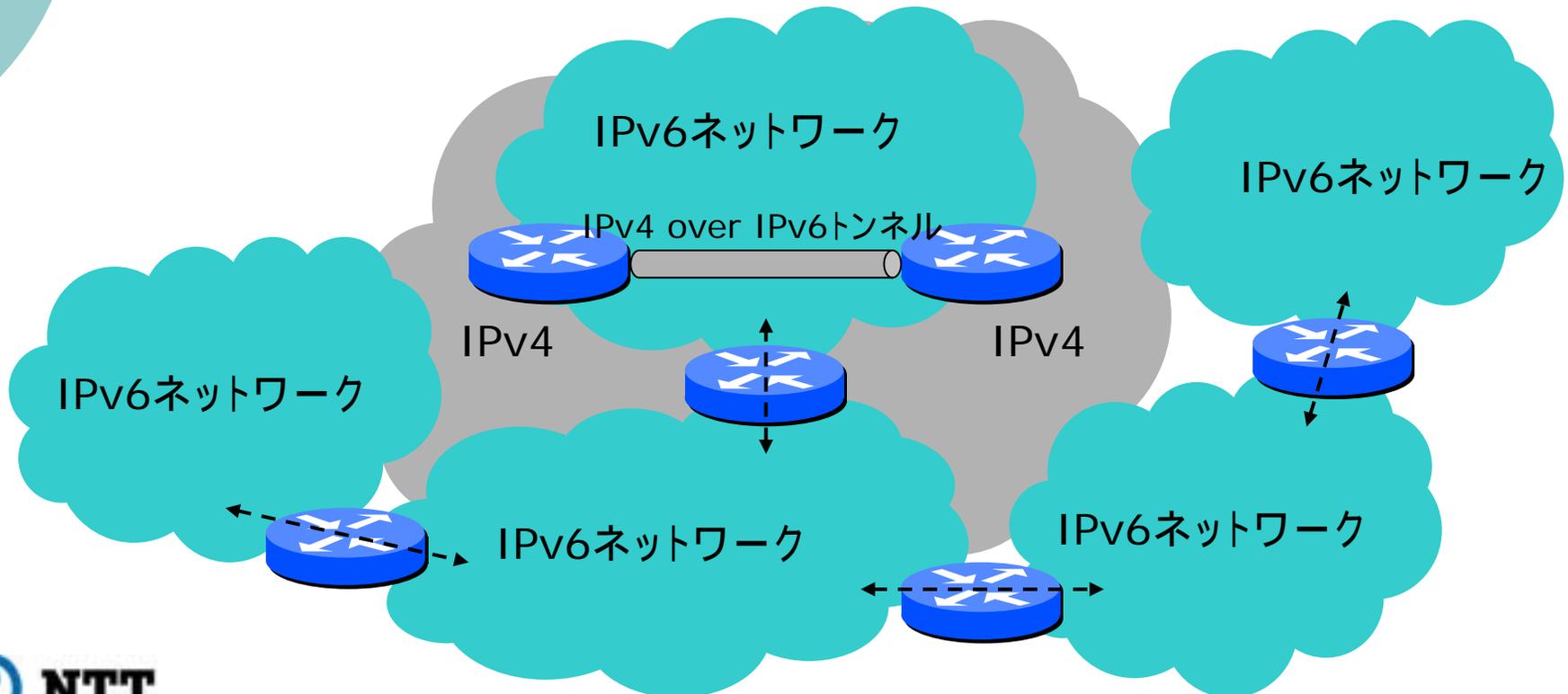
移行シナリオ (第2段階)

- IPv4ネットワーク IPv6ネットワークの時
 - ネイティブなIPv6ネットワーク構築



移行シナリオ (第3段階)

- IPv6ネットワーク >> IPv4ネットワークの時
 - IPv4 over IPv6トンネリングによるネットワーク構築



IPv6実験ネットワーク

○ 国際的実験ネットワーク

- 6bone

- IPv6の Protokol 設計段階から運用されているネットワーク
- 実験用アドレスブロック pseudo-TLA (pTLA) を割り振っている
- IPv6の Protokol 仕様の検証、各実装の相互接続性の検証、運用技術の実証に貢献
- 2004年1月1日に pTLA 新規アドレス割振りを停止、2006年6月6日以降に pTLA アドレス運用停止

○ 国内の実験ネットワーク

- 6bone-jp

- 6boneと接続する日本最初のIPv6ネットワーク
- 実験用アドレスブロック NLA を割り振っている

- NSPIXP-6

- 1999年8月に運用開始された日本初のIPv6 IX (インターネット相互接続点)
- IPv6基幹ネットワークのための基盤を提供

IPv6アクセスサービスの現状

○ 商用サービス(7社)

- NTTコミュニケーションズ
- IIJ
- パワードコム
- 日本テレコム
- ニフティ
- KDDI
- JENS

○ 試行サービス(9社)

- NTT東日本
- ドリーム・トレイン・インターネット
- 知多メディアスネットワーク
- メディアエクスチェンジ
- STNet
- 北陸通信ネットワーク
- Panasonic
- フリービット
- 日本サステイナブル・コミュニティ・センター

IPv6基幹サービスの現状

- 世界各国のIXでIPv6サービス開始済
 - 日本
 - NSPIXP6, NSPIXP2, JPNAP, JPIX
 - アジア
 - 6NGIX, XchangePoint
 - 北米
 - 6IIX, 6TAP, Florida-MIX, MCI MAE, NY6IX, PAIX, S-IX
 - 欧州
 - AMS-IX, FICIX, FNIX6, INXS, NaMeX, TREX, UK6X
- 北米、欧州のIXでIPv6対応が活発化

IPv6ポータル・サービス

- IPv6情報サイト
 - IPv6style
 - IPv6を知り、つくり、使う人たちのための総合情報サイト
 - IPv6start.net
 - 多くの人にIPv6の意義や役割, しくみや使い方を紹介するサイト
- IPv6関連団体
 - IPv6普及・高度化推進協議会
 - e-Japanの重点計画である安全・迅速・簡単に行えるIPv6インターネット環境の実現を目指す団体

IPv4は使えなくなるのか？

- IPv4は徐々にIPv6で置き換えられていくと考えられるが、IPv4が使えなくなるわけではない
- インターネットの基幹がIPv6に置き換えられてもトンネリングなどを用いて通信することは可能
- IPv6への移行はいずれ必ず行われるので、IPv4に特化しないサービス・ネットワーク運用を視野に入れておく必要はある

本日の内容

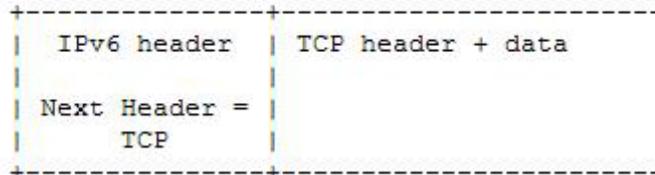
- IPv6のこれまで
 - 誕生の歴史
 - 基本的仕様と機能
 - **拡張的仕様と機能**
- IPv6のこれから
 - 関連する新しい仕様
 - ユビキタス・ネットワークの話

セキュリティやモビリティ、リアルタイム性確保等の機能の標準実装

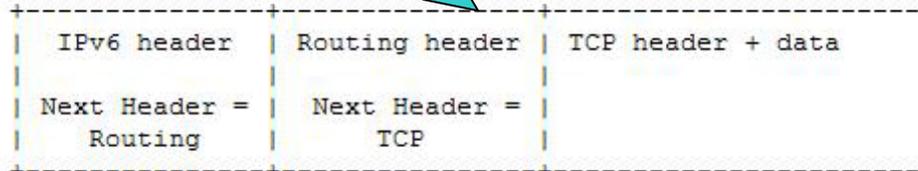
- 柔軟な機能拡張を可能にする技術
 - 拡張ヘッダ
- 特徴的な機能
 - セキュリティ: IPsec、匿名アドレス
 - モビリティ: MobileIPv6
 - リアルタイム性確保: QoS制御

IPv6の拡張ヘッダ

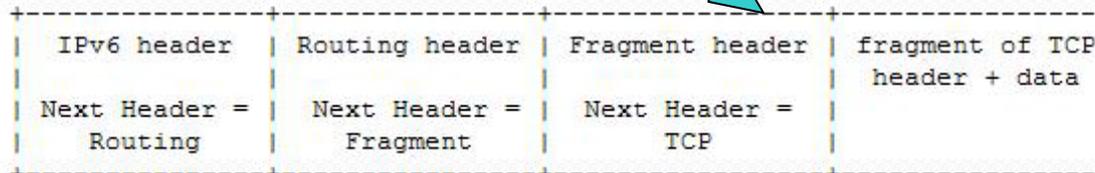
- 拡張ヘッダの組み合わせで機能を実現し柔軟性を向上
- サイズを固定化し処理負荷を軽減



← 拡張ヘッダの挿入



← 拡張ヘッダの挿入



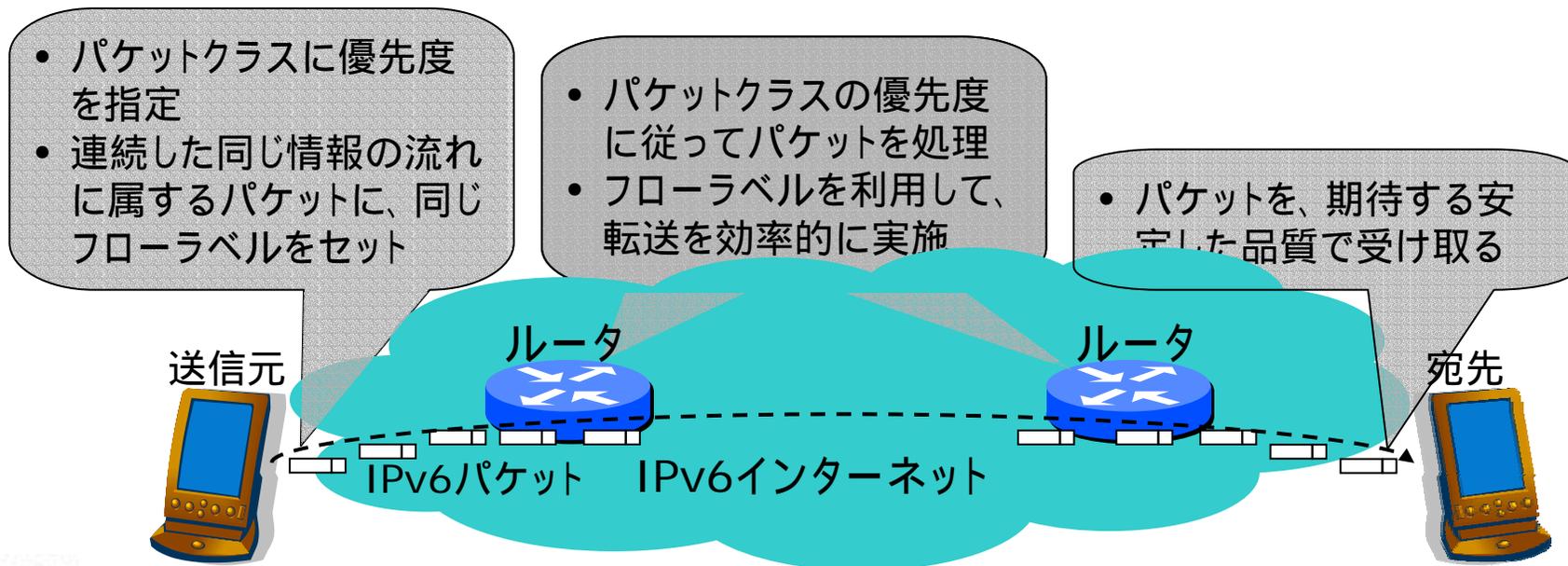
拡張ヘッダの種類と順序 (RFC2460)

1. ホップバイホップオプションヘッダ
 - 経路上のすべてのノードで処理される情報
2. ルーティングヘッダ
 - 送信元から宛先までの中継ノードリスト
3. フラグメント化ヘッダ
 - 送信元におけるパケット分割の際の情報
4. 認証ヘッダ (AH)
 - パケットの認証情報
5. 暗号ペイロードヘッダ (ESP)
 - パケットの暗号化情報
6. 宛先オプションヘッダ
 - 宛先においてのみ有効なオプション
 - MobileIPv6で使われるHome address optionなど

リアルタイム性確保: QoS制御

○ 提供する機能

- クラスとフローラベルを設定することにより、ルータで優先順制御を可能にし、遅延やそのゆらぎの小さな高品質なネットワーク環境を実現する



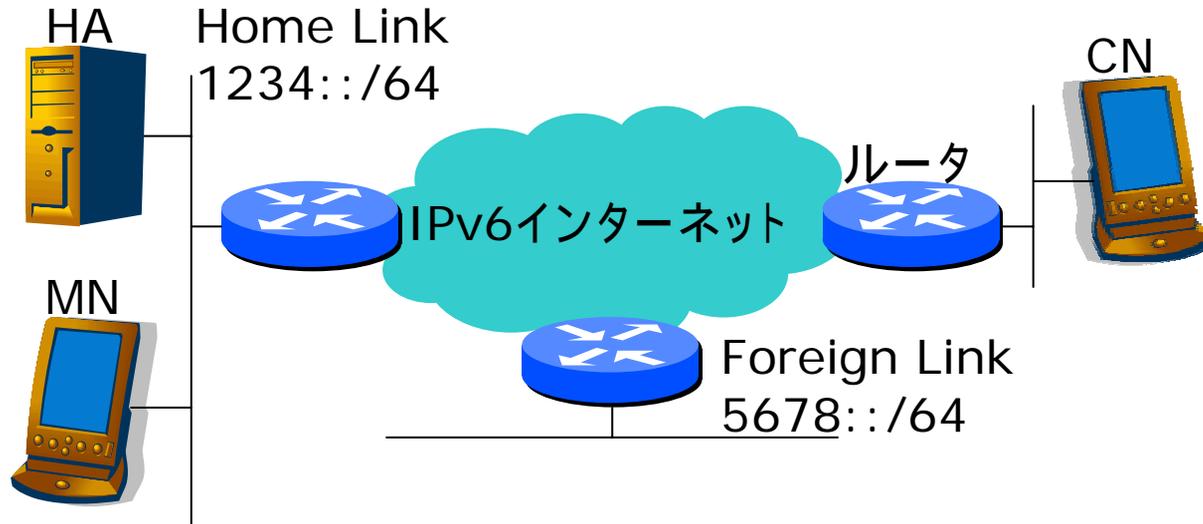
モビリティ: MobileIPv6

- 提供する機能
 - 継続中の通信を切断することなく移動を実現する
- 特徴
 - IPレイヤのみで実現
 - アプリケーション、レイヤ2のサポートが不要 (= 既存のアプリケーション、レイヤ2の改造が不要)
- Mobile IPv4との比較
 - 経路最適化が最初から考慮されている
 - Foreign Agentの廃止

Mobile IPv6の動作例(1)

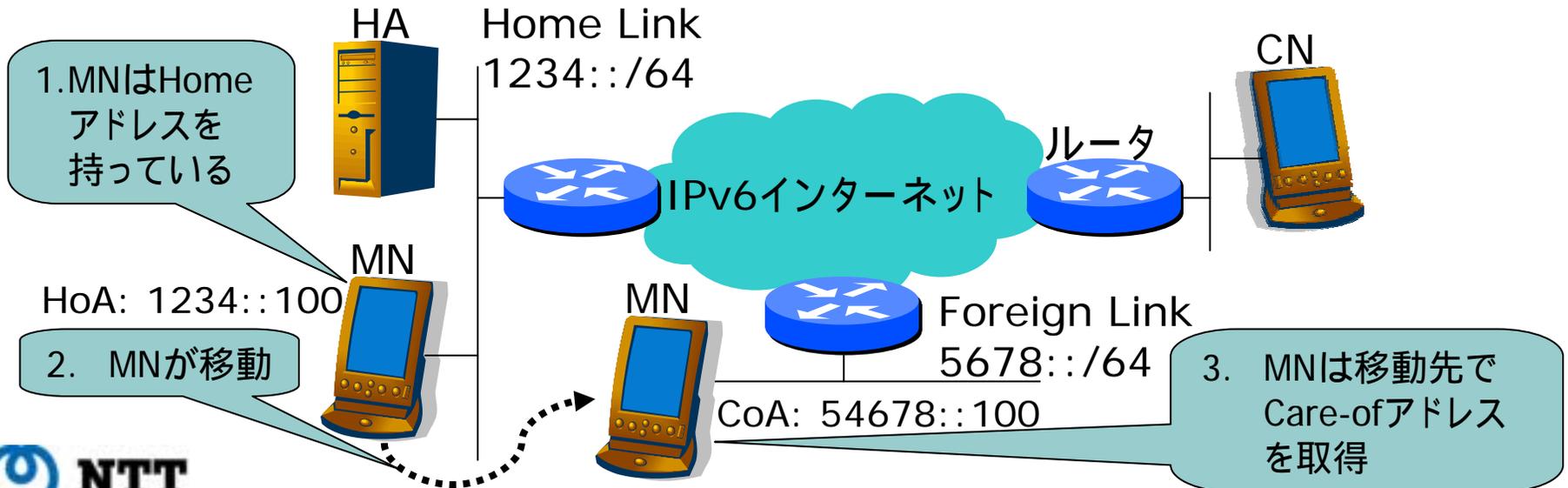
○ モバイルIPの専門用語

- Home Agent (HA) MNの移動先を登録するルータ
- Mobile Node (MN) 移動ノード
- Correspondent Node (CN) MNの通信相手
- Home Link (HL) MNのホームアドレスが登録されているリンク
- Foreign Link (FL) MNの移動先のリンク
- Home Address (HoA) ホームリンクにおけるMNのアドレス
- Care-of Address (CoA) FLにおけるMNのアドレス
- Binding Cache ホームアドレスとcare-ofアドレスの対



Mobile IPv6の動作例(2)

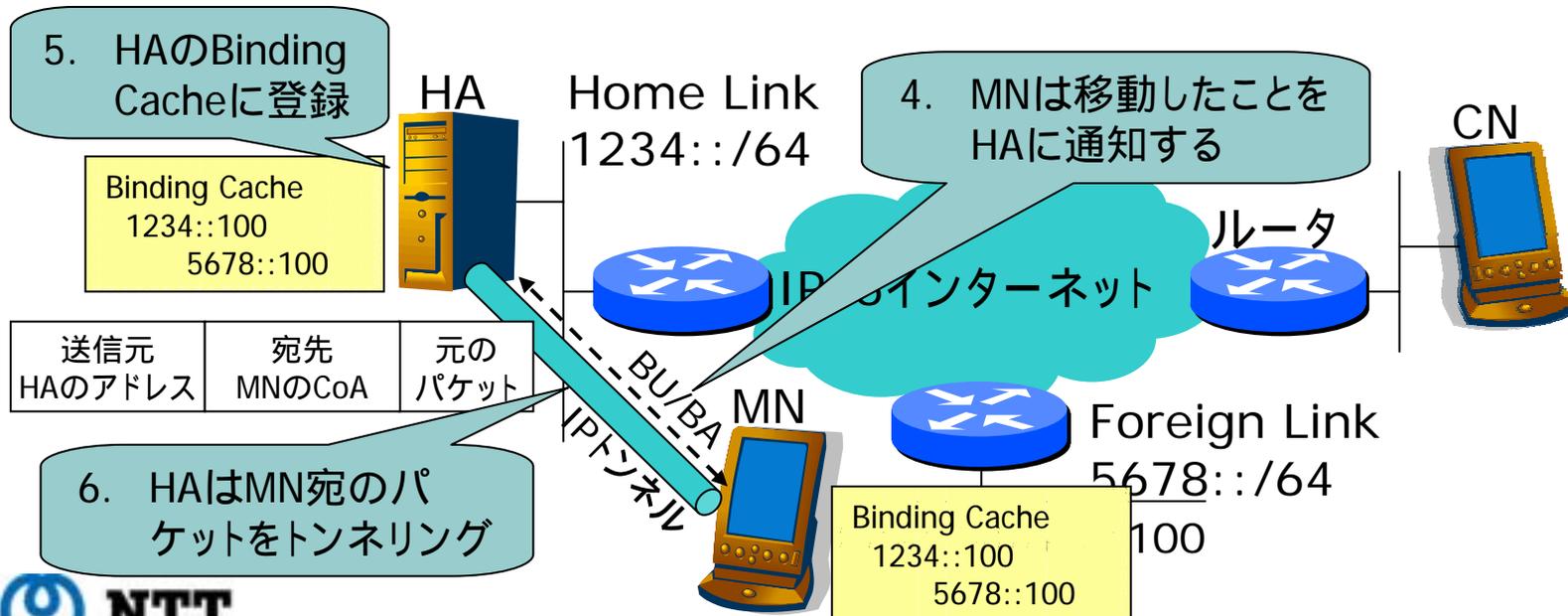
1. MNにHomeアドレスを設定
2. MNはForeignリンクへ移動
3. ForeignリンクのルータからCare-ofアドレスを取得



Mobile IPv6の動作例(3)

このままではCNとの通信がとぎれてしまうので

4. MNはHAにBinding情報を知らせるため、Binding Update (BU)、Binding Acknowledgement (BA) パケットを送受信
5. HAのBinding CacheにMNのCare-ofアドレス情報を登録
6. HAを経由したトンネル転送



セキュリティ: 匿名アドレス (RFC3041)

○ 解決する課題

- ステートレス・アドレス自動設定により設定されるIPv6アドレスは通常同一になるため、第3者のトラッキングが可能になる

○ 提供する機能

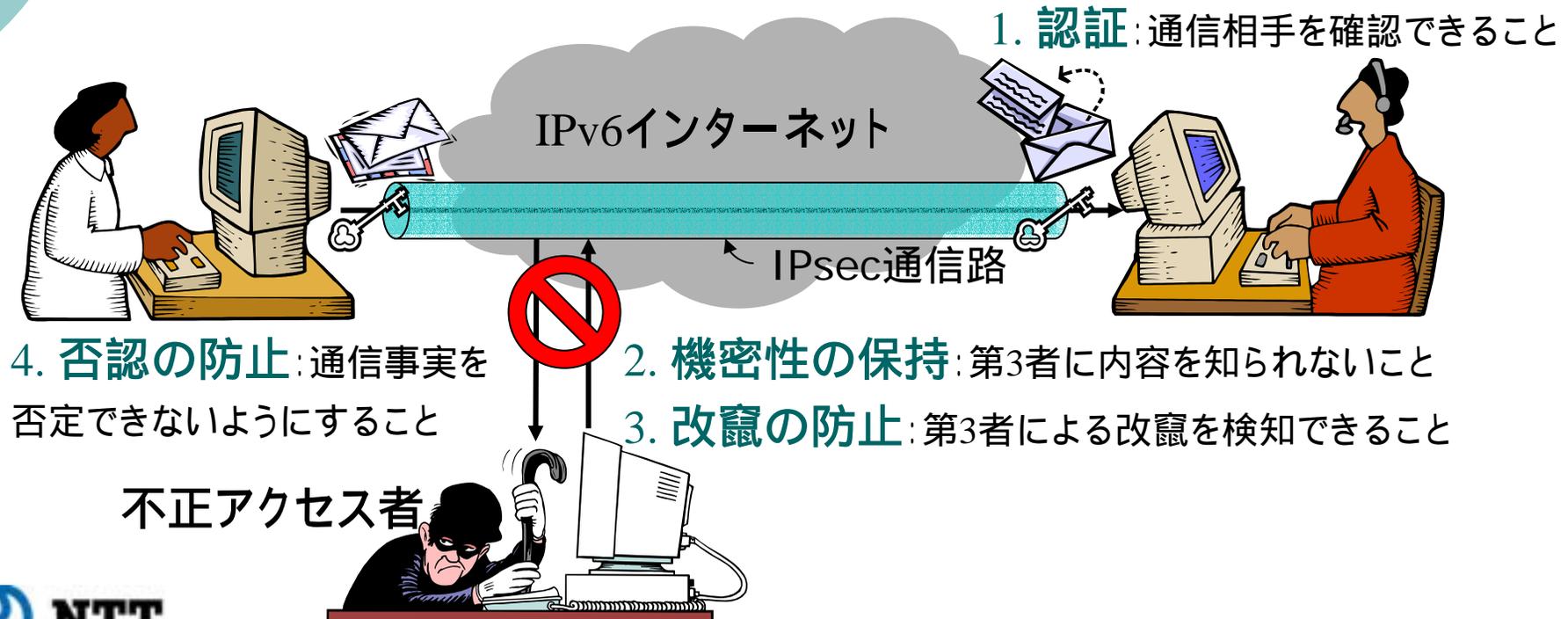
- インタフェースIDをEUI-64アドレスからランダムに生成
- 定期的(24時間程度)にアドレスを変更

○ 注意点

- クライアント向け(DNSやメールサーバには不向き)
- UDPアプリケーションには使いづらい

セキュリティ:IPsec

- インターネットをあたかも専用線のように安全な通信路として利用可能にする技術
- インターネットの基本プロトコルレベルで4機能を実現



IPsecの基本機能

- 認証ヘッダ (AH)
 - 改竄の防止、認証、否認の防止
 - デフォルトアルゴリズム: MD5
- 暗号化ペイロードヘッダ (ESP)
 - 機密性の保持
 - デフォルトアルゴリズム: DES

⇒ パケット単位でのセキュリティ機能を実現



SPI: Security Parameter Index

IPv6 IPsecのパケット形式

○ IPsecプロトコル

- トランスポートモード: End-to-End向け
- トンネルモード: Site-to-Site向け

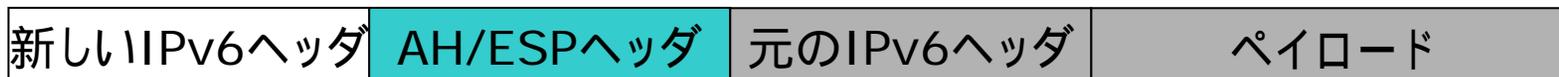
通常のIPv6パケット



トランスポートモードのIPv6 IPsecパケット



トンネルモードのIPv6 IPsecパケット



宛先: トンネル出口

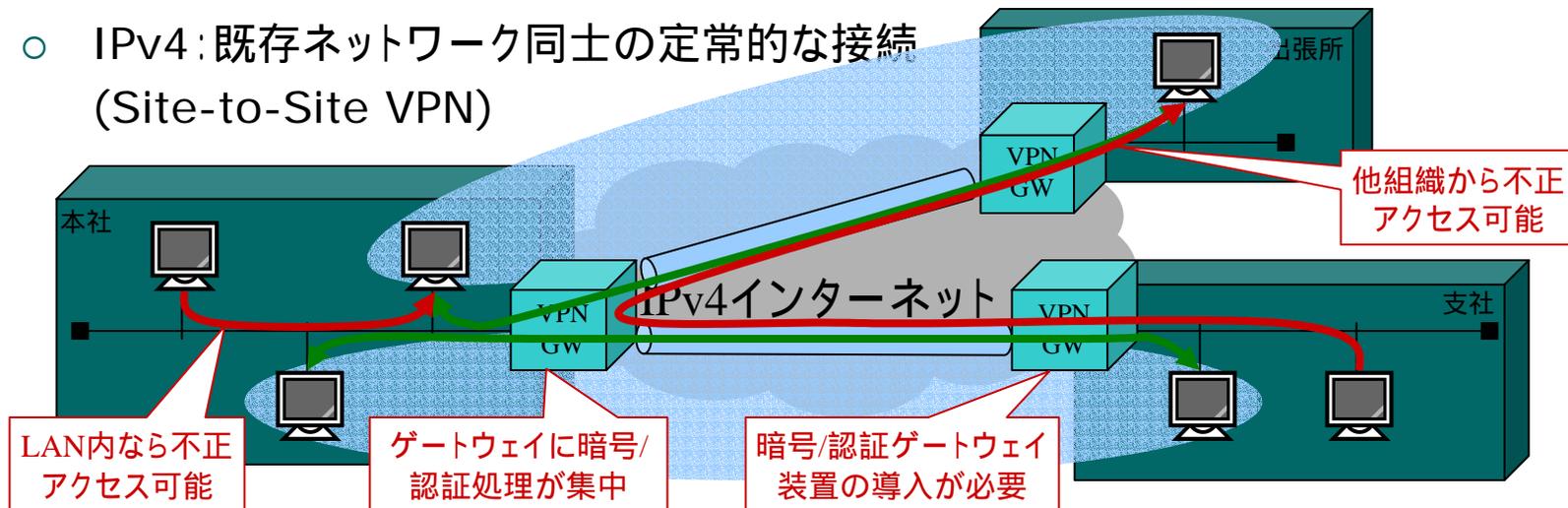
IPv6におけるIPSecの特徴

- 全ノードがIPSecによるセキュア通信可能
 - 高価なセキュリティGWが不要になる
IPv6の必須セキュリティ機能(IPSec)
- End-to-Endで通信可能
 - ホスト単位でVPN参加者を制御できる
IPv6の豊富なグローバルアドレス空間
- NAT不要のため、IPSec機能への制約がない
 - 任意のホストをVPNメンバに指定可能
IPv6の豊富なグローバルアドレス空間

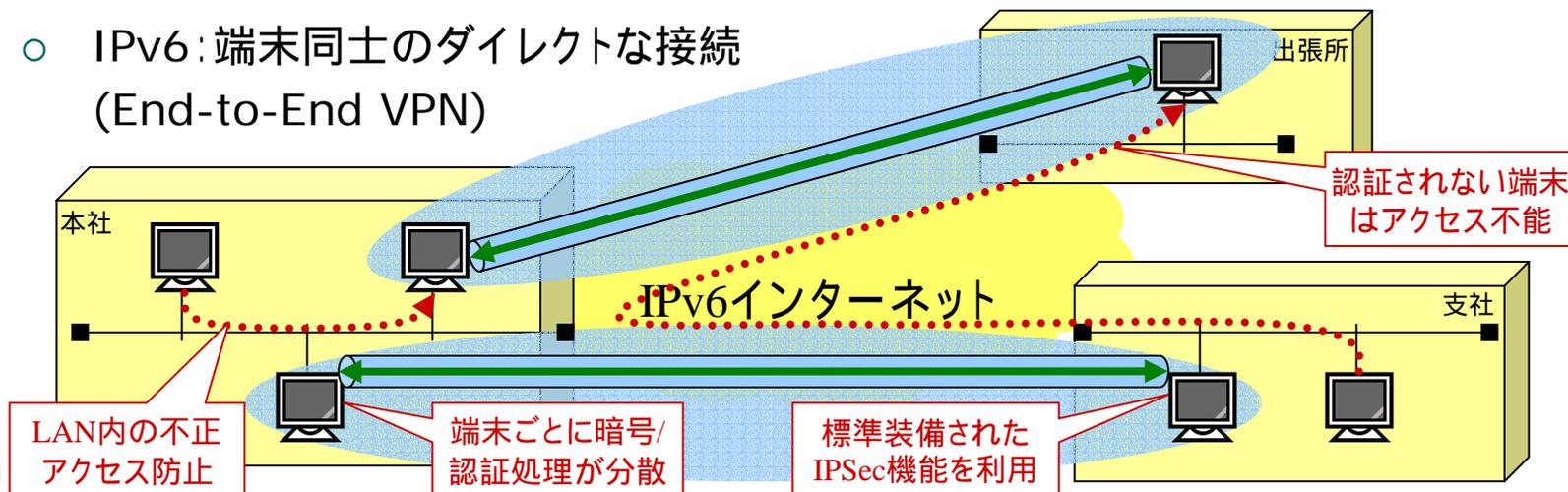
セキュアネットワーク利用形態の比較

～ IPv4 vs. IPv6 ～

- IPv4: 既存ネットワーク同士の定常的な接続 (Site-to-Site VPN)



- IPv6: 端末同士の直接的な接続 (End-to-End VPN)



End-to-End VPNの特徴

○ 長所

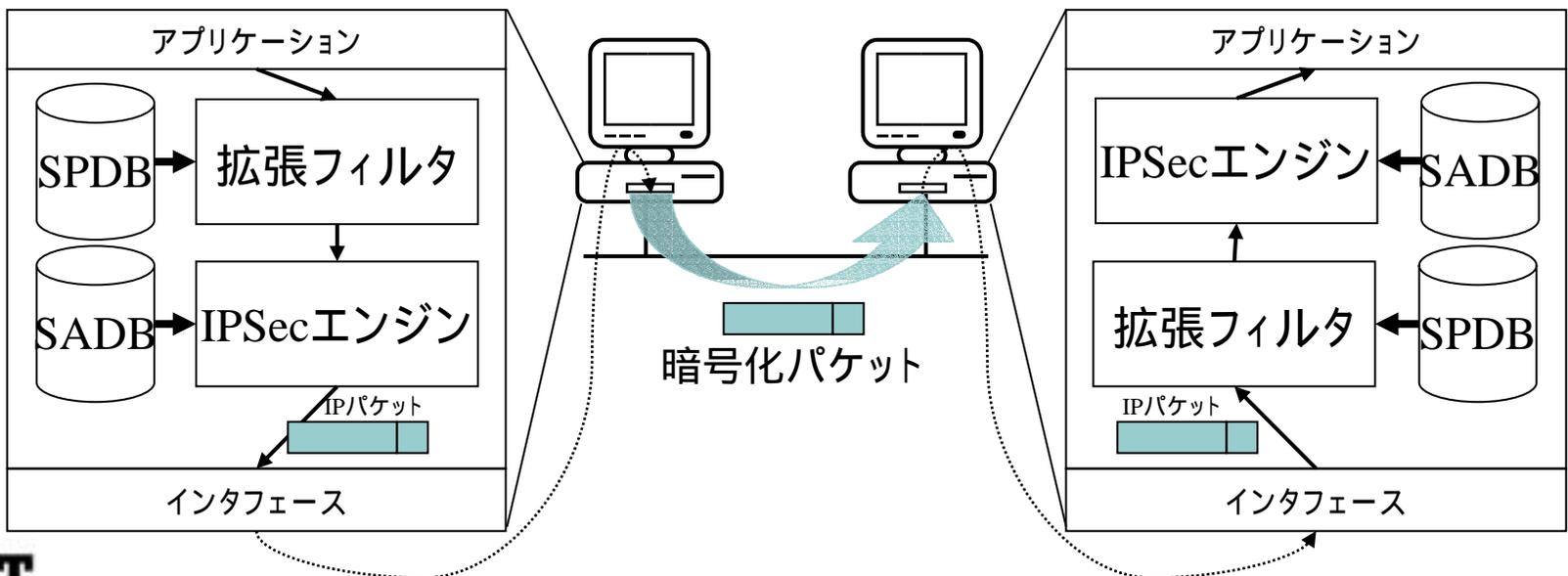
- 高性能なセキュアGWが不要になるので、コストを抑えられる
- ホスト単位でVPNに加入 or 非加入を決定できる
 - 1ホストだけを外部からアクセス可能に
 - 1ホストが複数の異なるVPNにアクセス可能に

○ 短所

- ホストに暗号処理の負荷がかかる
 1. マシン性能の向上で解決可能
 2. 分散処理効果がある(ネットワーク全体性能はホスト性能の和)
- VPN設定のためにホスト毎の設定が必要となる
インターネット鍵交換プロトコルによる自動設定が重要

IPSec機能とその動作

- IPSecプロトコルの処理構造と設定データ
 - IPSec通信の適用/不適用を決定するポリシ・データベース
 - セキュリティポリシ・データベース(SPDB)
 - IPSec通信の暗号化・復号化に必要な鍵データベース
 - セキュリティアソシエーション・データベース(SADB)



インターネット鍵交換プロトコルとは

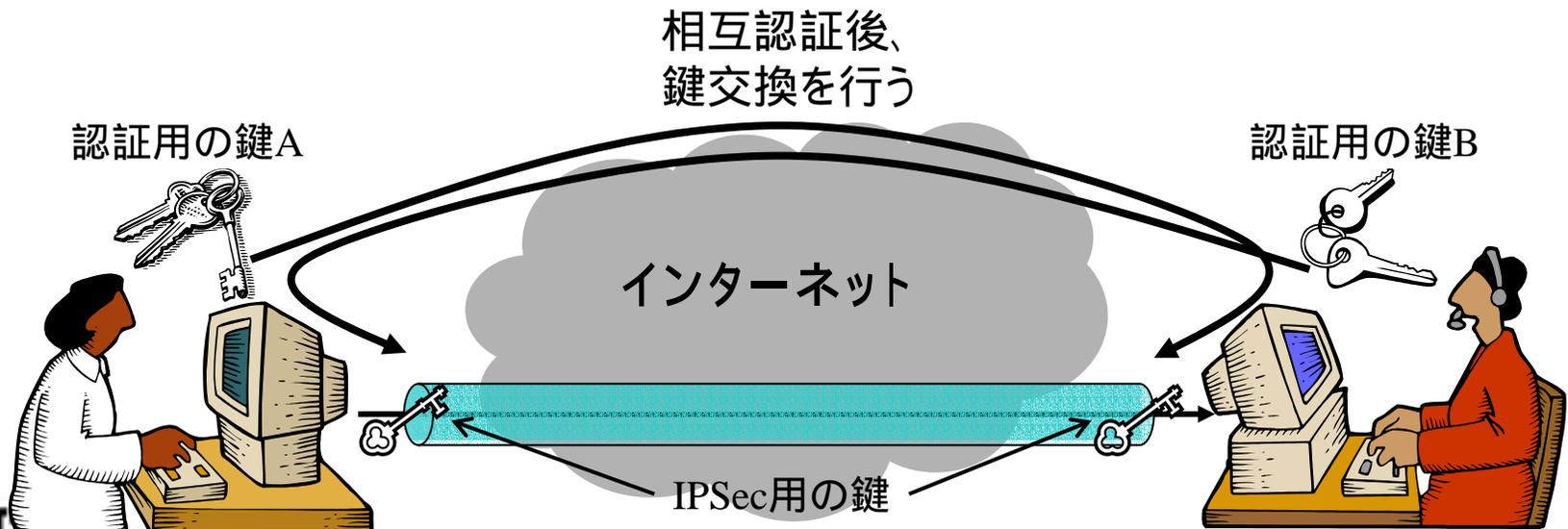
○ 目的

- 多くの端末とIPSec通信を行う場合でも、自動的に鍵を交換して、簡便にIPSec通信を行えるようにする

○ 相互認証方式

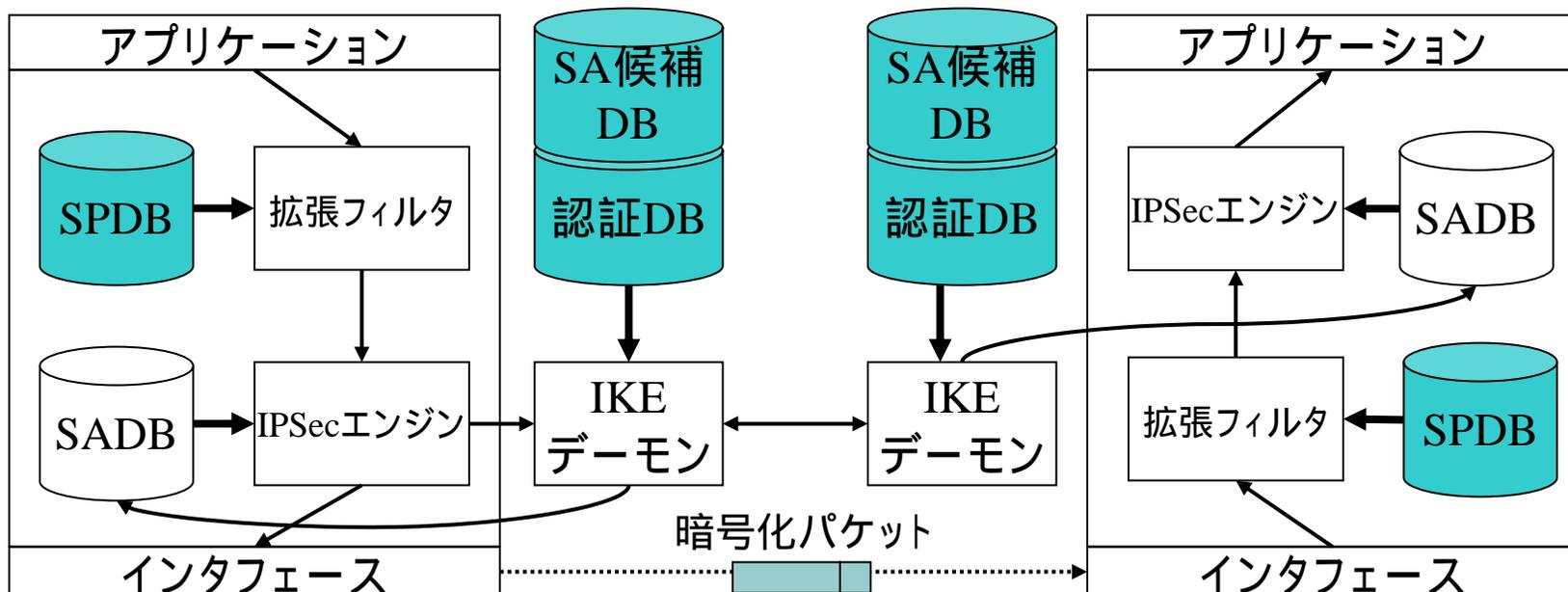
- 既知共有秘密鍵: 事前共有秘密鍵で認証
- デジタル署名: 公開鍵を使った署名で認証
- 公開鍵暗号: 公開鍵を使った暗号文で認証

→ インターネットだけを介した認証が可能

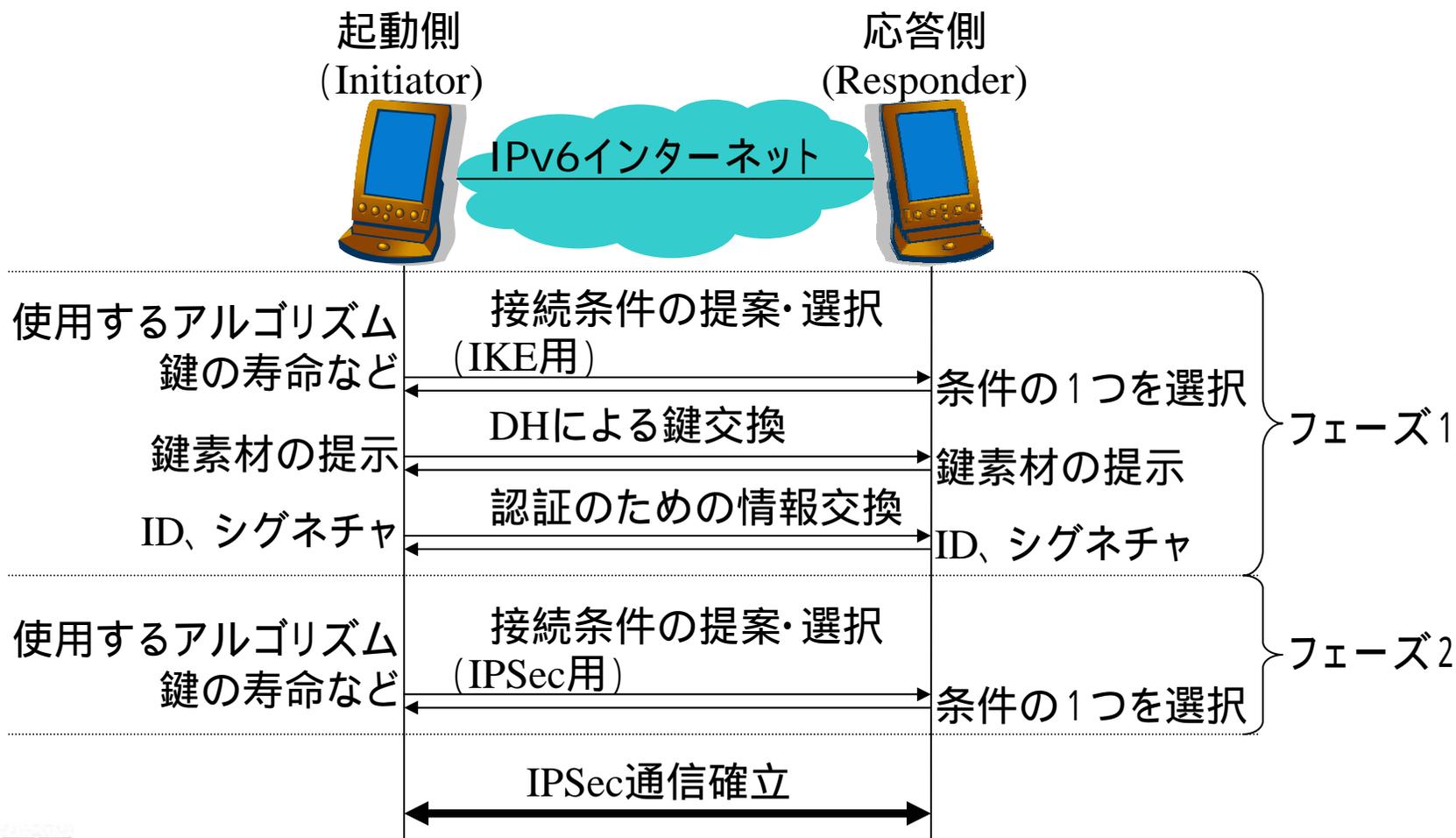


インターネット鍵交換機能

- インターネット鍵交換 (IKE) プロトコルの処理構造と設定データ
 - 鍵 (SA) が無いときに起動して、通信者間で SA を交換する
 - SA 候補群のデータベース
 - 通信相手のなりすましを防ぐために認証を行う
 - 認証データベース



インターネット鍵交換の動作



IPv6 IPsec の課題と研究動向

○ 課題

- プラグ&プレイが困難な設定の煩雑さ
- 非PCデバイスにおける暗号処理の負荷

○ 研究動向

- 次世代鍵交換プロトコル
 - IKEv2 (Internet Key Exchange version 2)
 - KINK (Kerberized Internet Negotiation of Keys)
 - PnP IPsec (Plug and Play IPsec)
- 暗号処理の改良や検討
 - AES (Advanced Encryption Standard)
 - LCNA (Low Cost Network Appliance)

IPsec関連RFC

- IPセキュリティ・アーキテクチャ全般
 - RFC2401, 2411
- IPsecの認証機能、暗号化機能
 - RFC2402 ~ 2406, 2410, 2451
- 鍵交換機能
 - RFC2407 ~ 2409, 2412

本日の内容

- IPv6のこれまで
 - 誕生の歴史
 - 基本的仕様と機能
 - 拡張的仕様と機能
- IPv6のこれから
 - **関連する新しい仕様**
 - ユビキタス・ネットワークの話

関連する新しい仕様

- 2002年以降のIPv6 RFC (Proposed Standardのみ)
 1. RFC3595: *Textual Conventions for IPv6 Flow Label*
 2. RFC3590: *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*
 3. RFC3513: *Internet Protocol Version 6 (IPv6) Addressing Architecture*
 4. RFC3484: *Default Address Selection for Internet Protocol version 6 (IPv6)*
 5. RFC3315: *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
 6. RFC3307: *Allocation Guidelines for IPv6 Multicast Addresses*
 7. RFC3306: *Unicast-Prefix-based IPv6 Multicast Addresses*
 8. RFC3266: *Support for IPv6 in Session Description Protocol (SDP)*

関連する新しい仕様

- 2002年以降のIPv6 RFC (Proposed Standardのみ)
 1. RFC3595: *Textual Conventions for IPv6 Flow Label*
 2. RFC3590: *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*
 3. RFC3513: *Internet Protocol Version 6 (IPv6) Addressing Architecture*
 4. RFC3484: *Default Address Selection for Internet Protocol version 6 (IPv6)*
 5. RFC3315: *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*
 6. RFC3307: *Allocation Guidelines for IPv6 Multicast Addresses*
 7. RFC3306: *Unicast-Prefix-based IPv6 Multicast Addresses*
 8. RFC3266: *Support for IPv6 in Session Description Protocol (SDP)*

RFC3513: *Internet Protocol Version 6 (IPv6)*

Addressing Architecture

- 内容
 - ユニキャスト、マルチキャスト、エニキャスト全てに関するIPv6アドレス体系の定義
- 旧仕様(RFC2373)からの主な変更点
 - インタフェース識別子の一意性を「リンク上」から「サブネットプレフィックス中」に変更
 - サブネット識別子フィールドを54ビットにしてサイトローカル形式を変更
 - フォーマットプレフィックス(FP)の除去
 - アドレス種別リストについて、グローバルユニキャストを例外とし、それ以外の全てを識別する形式へ変更
 - IPv4互換IPv6アドレスがグローバルIPv4ユニキャストアドレスを使わなくてはならない説明を追加
 - IPv4射影アドレスの定義を明確化
- 関連事項
 - サイトローカル形式の変更に伴い、サイトローカルアドレスが使用できなくなった。

RFC3484: *Default Address Selection for Internet Protocol version 6 (IPv6)*

- 内容
 - 複数のユニキャストアドレスがインタフェースに割り当てられている場合に、送信元アドレス、宛先アドレスを選択する方法を規定
- 複数のアドレスがインタフェースに割り当てれる場合
 - インターネット接続ホスト: リンクローカルアドレスとグローバルアドレス
 - 匿名アドレス: 公共アドレスと一時アドレス
 - MobileIPv6移動ノード: ホームアドレスと気付けアドレス
 - マルチホーム接続ホスト: ISP A用アドレスとISP B用アドレス
 - マルチインタフェースホスト: I/F AアドレスとI/F Bアドレス
 - トンネル接続ホスト: I/Fアドレスと擬似I/Fアドレス
 - デュアルスタックホスト: IPv6アドレスとIPv4アドレス
- 関連事項
 - サイトマルチホームに関する議論は、multi6 WGで議論中
 - プログラミング時のgetaddrinfo関数の返値の取扱いに注意が必要

RFC3315: *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

○ 概要

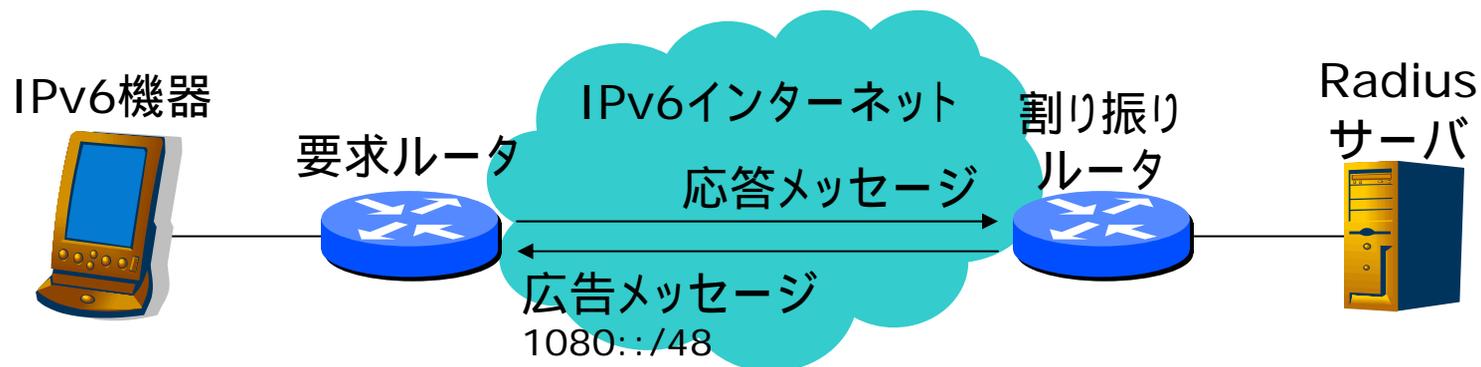
- DHCPサーバがIPv6ノードにIPv6ネットワークアドレスのような設定パラメータを渡す方法を定義

○ ポイント

- ステートレスアドレス自動設定プロトコルとの併用が可能
 - DNSアドレス通知など

○ 関連事項

- プレフィックス割り振りオプションを議論中



その他のRFC概要

- RFC3595: Textual Conventions for IPv6 Flow Label
 - MIB(Management Information Base)に格納されているIPv6フローラベル情報を統一的に扱えるようにする変換機能の定義
- RFC3590: Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
 - 近隣探索プロトコルでマルチキャストを使って重複アドレスを発見する際に使用する送信元アドレスの選択方法に関する規定
- RFC3307: Allocation Guidelines for IPv6 Multicast Addresses
 - マルチキャストアドレスの衝突を防ぐための永続的マルチキャストアドレスの割当て、動的マルチキャストアドレスの確保、永続的マルチキャストグループの定義に関するガイドライン
- RFC3306: Unicast-Prefix-based IPv6 Multicast Addresses
 - ドメイン間のアドレス確保プロトコルを使わずに、マルチキャストアドレスを動的に確保できるようにするために、ユニキャストプレフィックスをグループIDに用いたマルチキャストアドレス決定方法の定義
- RFC3266: Support for IPv6 in Session Description Protocol (SDP)
 - セッション記述プロトコル(RFC2327)に対するIPv6アドレス文法の追加定義

本日の内容

- IPv6のこれまで
 - 誕生の歴史
 - 基本的仕様と機能
 - 拡張的仕様と機能
- IPv6のこれから
 - 関連する新しい仕様
 - **ユビキタス・ネットワークの話**

ユビキタス・ネットワークの話

- ユビキタスとは、
 - 同時に、どこにでもあること。
 - コンピューターを意識することなく現実生活のいたるところで利用できるような環境という意味でユビキタス-コンピューティングなどが注目されている
- ユビキタス・ネットワークとは、
 - どこにでもあるネットワーク、つまり、いつでも、どこでも、どんなものからでもネットワークにつながるという意味

IPv6の世界



第3、第4世代携帯電話

- 活動概要
 - 3GPP(The 3rd Generation Partnership Project)において、IPを用いた高速通信や音声通話に関する技術を検討中
- IPv6との関連
 - IETF IPv6 WGが3GPPにおけるIPv6利用方法に関するInformational RFCを提出
- 関連ニュース
 - 2003年1月31日
 - IPv6を使用した3G UMTS/WCDMAネットワークのデモを実施(エリクソン)
 - 2003年3月14日
 - MobileIPv6対応セキュア携帯情報端末(ノキアジャパン & NTTコミュニケーションズ)

ITS (Intelligent Transport System)

○ 活動概要

- 道路交通が抱える事故や渋滞、環境対策など、様々な問題を「情報化」と「知能化」により抜本的に解決する
- ITSは人と道路と自動車の中で情報の受発信をするシステム

○ IPv6との関連

- インターネットITSプロジェクトの実証実験にIPv6を利用
- IPv6普及・高度化推進協議会が、トレインモバイルSGにおいて、インターネットITSと連携

○ 関連ニュース

- 2001年10月18日
 - インターネットITSプロジェクト、IPv6を用いた車両2000台規模の実証実験

情報家電

○ 活動概要

- Echonet、NonPCインターネットコンソーシアムなどの団体や各企業が独自に開発を進行中
- リモートセキュリティ関連、AV & ゲーム関連などを用いた実験が活発

○ IPv6との関連

- Echonet規格検討においてIPv6対応を検討中
- ネットワークカメラ、PDA、デジタルカメラなどのIPv6接続実験

○ 関連ニュース

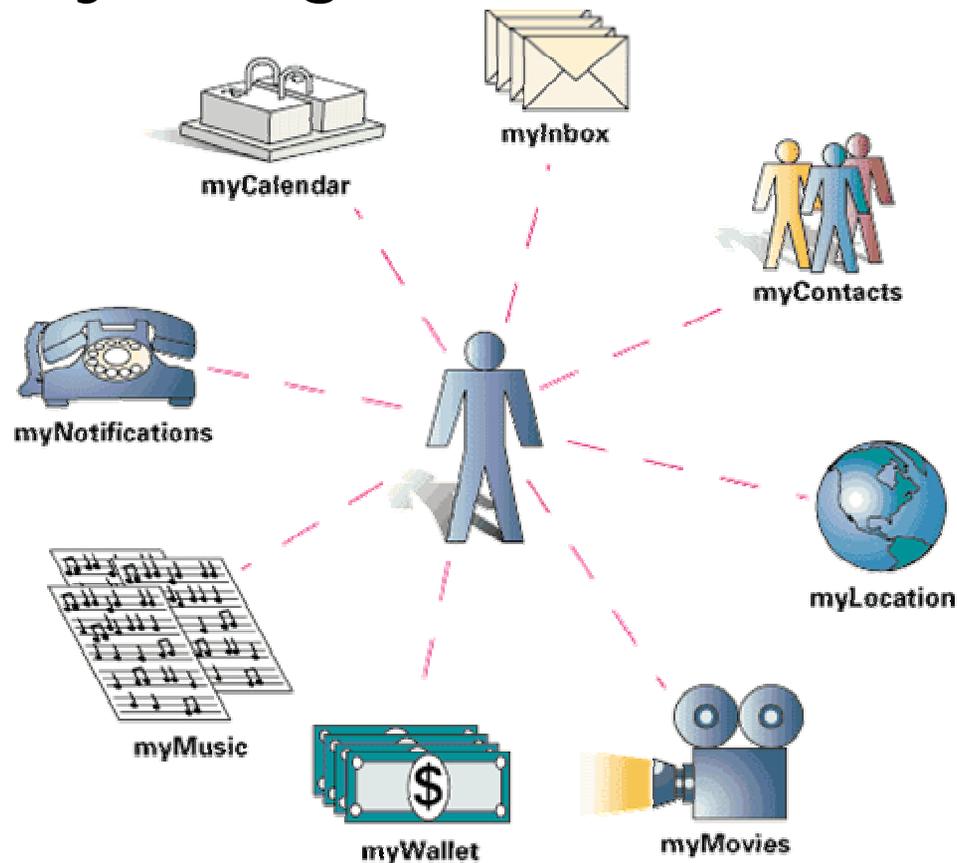
- 2003年10月21日
 - IPv6家庭内ネットワーク機器の相互接続仕様を策定(日立と松下)
- 2003年10月30日
 - NonPCインターネットコンソーシアム、IPv6対応ネット家電の接続実証実験を実施

AutoIDセンタ

- 活動概要
 - マサチューセッツ工科大学に本部を置く非営利団体
 - グローバルなサプライチェーン上での製品識別とトラッキングを可能にするインフラの構築と標準化を行う
- IPv6との関連
 - オートIDセンターなどに代表されるRFIDシステムは、IPv6と同様にインターネットマーケットを拡大する新しいインターネット活用技術として期待されている
 - IPv6アドレスを持つモノ同士が交信するエンド・ツー・エンドのアプリケーションが出現すると、オートIDによってモノの意味を知らせることが重要となる
- 関連ニュース
 - 2003年1月22日
 - オートIDセンター日本拠点、慶應SFC内に開設
 - 2003年6月30日
 - 松下電器やNEC, 日立など8社, 「IPv6センサネットワークングコンソーシアム」を設立
 - 2003年10月23日
 - オートIDセンターの標準に準拠したネットワーク利用型RFIDシステムの開発完了と実証実験の開始について

まとめ

- Every thing over IP around me



2003年 IPv6ニュース1 (6月16日)

○ 米国防総省、IPv6を採用へ



● 主催

○ 米国防総省

● 目的

○ Defense Transformation

- <http://www.usipv6.com/ppt/ipv6keynotesummit.pdf>

● 内容(Global Information Grid(GIG))

- 2003年10月より、同省のネットワーク関連調達案件については、IPv6へ対応していることと
- 2008年にはIPv6に完全移行することを目標

● 効果

- IPv6への追い風? 逆風?と両見解あり

2003年 IPv6ニュース2(9月24日)

- IPv6アプリコンテスト2003開催 (<http://www.v6pc.jp/apc/jp/invitation.html>)
 - 主催
 - IPv6普及・高度化推進協議会
 - 目的
 - インターネットの新しい利用シーンを創造する様々な分野のアプリケーションやソフトウェアを選奨し表彰する
 - 受賞
 - インプリ部門グランプリ
 - 着目点の多地点間での遠隔共有ツール
 - インプリ部門優秀賞
 - DV Conf、CyberLink IPv6 for Java、Conference over IP、IPv6 Monitoring Tool、HiMIPv6 (Hierarchical Mobile IPv6)
 - アイデア部門奨励賞
 - MIDI Composition To Copyright Tool for IPv6 (MC2C6)、Parking Control System with MIPv6、万歩計とIPv6によるお年寄の健康管理システム、家 in ZAURUS、Multicast peer to peer network

2003年 IPv6ニュース3(11月21日)

- 日中結ぶIPv6網が12月中旬にも開通(日経BP社)
 - 主催
 - 中国 国家発展改革委員会
 - 日本 経済産業省
 - 目的
 - ITSなどIPv6実験ネットワークの構築
 - ネットワーク施設協力企業
 - NEC
 - 日立製作所
 - 富士通
- 関連ニュース
 - COMM CHINAで“IPv6の日立”を中国で確立すると古川常務
 - 2002 IPv6 Forum Beijingに2000人の参加者

2003年 IPv6ニュース4(11月20日)

○ Panasonic hi-hoが、人類初の南極皆既日食中継をIPv6で配信

Panasonic hi-hoリリース(http://town.hi-ho.ne.jp/news_release/2003/1120.htm)より

- 主催
 - ライブ! ユニバース
- 目的
 - hi-hoによるIPv6への取り組み強化の一環
- 内容
 - 2003年11月24日6:40～8:00に南極「Shackleton Ice Shelf」の映像をWindows Mediaを使って配信

2003年 IPv6ニュース5(10月30日)

- ソフトフロント、NonPCインターネットコンソーシアムにIPv6対応SIP技術を提供

Softfront News(<http://www.softfront.co.jp/news/caverage/r-031030.html>)より

- 目的

- 今後SIP技術が活用される市場として最も拡大が期待されるネット家電分野に対し、SIP技術を提供することにより、ユビキタス社会の到来に際して当社のSIP技術がより多くの場面で利用される可能性が高まるものと期待

- 内容

- NonPC機器実証実験事業に対して『IPv6対応のSIPサーバーとクライアントソフト』を提供

2003年 IPv6ニュース6(10月21日)

- 日立と松下電器が共同でIPv6家庭内ネットワーク機器の相互接続仕様を策定し、新たなIPv6アーキテクチャを開発

日立ニュースリリース(<http://www.hitachi.co.jp/New/cnews/031021.html>)より

- 要旨

- 高度なセキュリティ性を有する次世代インターネットプロトコルであるIPv6を、異なるメーカーの情報家電や宅内機器などの家庭内ネットワーク機器間で利用するための相互接続の仕様を策定

- 内容

- IPv6を家庭内ネットワーク機器に適用する際の相互接続仕様の策定
 - IPv6の豊富なオプション(パケットサイズの調整、暗号・認証アルゴリズムの種類等)に対してホームネットワークで利用するための相互接続仕様を策定することによって、この仕様に基づいた家庭内ネットワーク機器であれば、異なるメーカー間であっても相互接続が可能
- 家庭内ネットワーク機器に適用可能なIPv6アーキテクチャの開発
 - IPv6処理を、CPUによるソフトウェア処理とコプロセッサによるハードウェア処理とに最適に機能分割することによって、全てをソフトウェアで処理した場合に比べて10倍以上の高速化ができ、低価格なCPUで高速な通信が実現できるため、機器の低価格化が可能。そのため、CPU性能やメモリ容量などのリソースに制限があり、コスト要求が厳しいIP電話などのコミュニケーション機器に適用が可能

2003年 IPv6ニュース7(10月1日)

○ 業界初、100Mbpsネット家電向けIPv6モジュールを開発

Panasonic News Release (<http://matsushita.co.jp/corp/news/official.data/data.dir/jn031001-2/jn031001-2.html>) より

● 要旨

- 家電機器のようなプログラムを格納するメモリサイズが小さく、また性能が低いCPUにも対応できるIPv6モジュールを開発
- ネット家電向けとして業界で初めて100Mbpsを実現し、プログラムサイズも業界最小レベル

● 内容

- ネット家電向けのIPv6機能の抽出およびカスタマイズを行う
ネット家電向けIPv6最適化技術
- CPUに負荷をかけずに通信の暗号処理を高速に行う、IP通信
アクセラレータ技術

2003年 IPv6ニュース8(9月2日)

○ ユビキタス時代に対応したビル環境マネジメントシステムをIPv6の採用で実現

清水建設ニュースリリース(http://www.shimz.co.jp/news_release/548.html)より

● 要旨

- 次世代のインターネット技術であるIPv6を用いて、ビル内のさまざまな設備・機器を効率的にしかもきめ細かく制御し、より一層快適な室内環境を実現する総合的ビル環境マネジメントシステムを開発

● 内容

- 汎用IPv6用端末装置を組み合わせた、次世代インターネット対応の総合的ビル環境制御システムにより、空調、照明、温・湿度、鍵制御システムなどを一つのシステムにまとめることが可能
- 高いセキュリティを保ちながらインターネットに接続できるIPv6技術を用いたことで、ビル館内の照明の一台、空調の一台にまでIPアドレスを付与し、これらをインターネットの通信プロトコルで個別に管理・制御