IPv6の現状

アラクサラネットワークス株式会社
鈴木伸介 <suz@alaxala.net>

AlaxalA
For The Guaranteed Network

概要

- IPv6仕様の現状
- IPv6運用の現状
- IPv6実装の現状
- まとめ

IPv6仕様の現状（基本仕様）

・IPv6検討開始時点から議論してきた基本仕様はほぼfix

プロトコルの微修正・RFCの格上げなどで、RFC番号が変更されているが、本質的内容はあまり変わっていない

・仕様適合性検証ツールもある

・IPv6 Ready Logo (http://www.ipv6ready.org/)

・商用のテストツール

・IETFでのプロトコル標準化にあたっては「IPv6対応」が強く要求される

新規プロトコルでのIPv6考慮漏れはまずない

IPv6仕様の現状 (基本仕様, cont.)

2006年7月以降に発行されたIPv6基本仕様関連RFC

RFC番号	タイトル	備考
4620	Node Information Query	ICMPで端末情報を取得
4773	IANAでの特殊目的IPv6アドレス管理	(事務手続を規定)
4861	NDP (改訂版)	RFC2461改訂版
4862	ステートレスアドレス自動設定 (改訂版)	RFC2462改訂版
4941	匿名アドレス (改訂版)	RFC3041改訂版
4943	NDP On-link Assumption廃止	RFC2461補足
5006	DNSサーバアドレス配布用RAオプション	RAでDNSサーバアドレス配布
5014	IPv6ソースアドレス選択API	
5072	IPv6 over PPP (改訂版)	RFC2472改訂版
5095	RH(Routing Header) Type 0の廃止	RH Type 0は、無制限に利用可能で危険なので、廃止
5156	特殊用途のIPv6アドレス一覧	
5172	IPv6CPデータ圧縮	RFC2472改訂版
5175	IPv6 RAフラグ拡張オプション	RAフラグのbit幅を拡張するオプション

IPv6仕様の現状（基本仕様以外）

・IPv6プロトコル設計の大筋は1990年代に決まった。
・それ以降の大きな潮流の変化は、基本仕様では必ずしもカバーできていない
　　インターネットのコモディティ化
　　脆弱性攻撃被害の甚大化
　　無線/携帯経由のインターネットの普及

→IPv6を拡張する仕様として規定
　・セキュリティ
　・無線系/モビリティ
　・マルチホーム

IPv6仕様の現状（セキュリティ関連）

NDP周りのセキュリティ技術標準化が多数行われてきた

IPsec&鍵交換ではカバーしきれないため

（鍵交換通信を行うためには、NS/NA解決が必要。

そもそもそのNS/NAを暗号化するために鍵交換している…）

代表的な技術

SEND (SEcuring Neighbor Discovery)　(RFC3971)

CGA (Cryptographically Generated Address)　(RFC3972)

RA Guard　　(draft-ietf-v6ops-ra-guard-00)

その他、実運用上課題になるIPv6固有なセキュリティ課題の整理が行われている。

代表的な技術

IPv6セキュリティ概論　(RFC4942)

ICMPv6フィルタリングガイドライン　(RFC4890)

アドレススキャン攻撃のインパクト　(RFC5157)

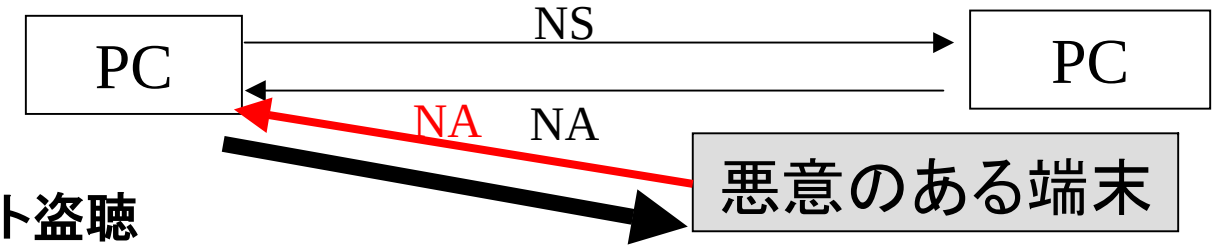
WIDE Secure6 WGの寄与

IPv6仕様の現状（セキュリティ関連）

NS/NA/RS/RAパケットを悪用すると何が出来るか?

・端末のなりすまし

NSに対して、本来の端末以外がNA応答



・パケット盗聴

ルータのふりをしてRA広告→全てのトラフィックがそこを経由

・通信不能

DAD応答を偽装することで、アドレス重複が起こったように見せかける

RAで、その網では使えないPrefix・デフォルトルータを広告

（特に後者は、悪意がないオペミスでも発生しうる）

IPv6仕様の現状（セキュリティ関連　---SEND---）

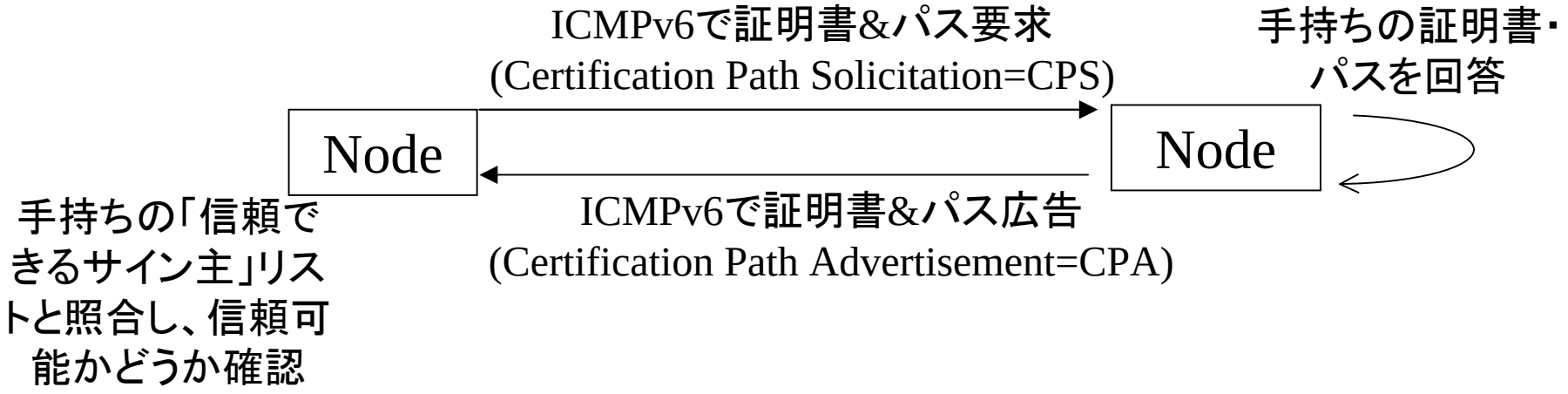
・NS/NA/RS/RAパケットに、認証情報を付加する

公開鍵

秘密鍵で計算した電子署名

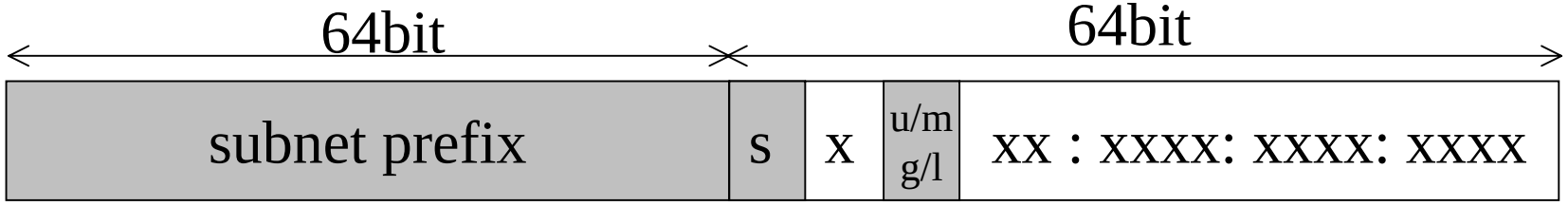
・上記2つを元に、「信頼できないNS/NA/RS/RA」を廃棄

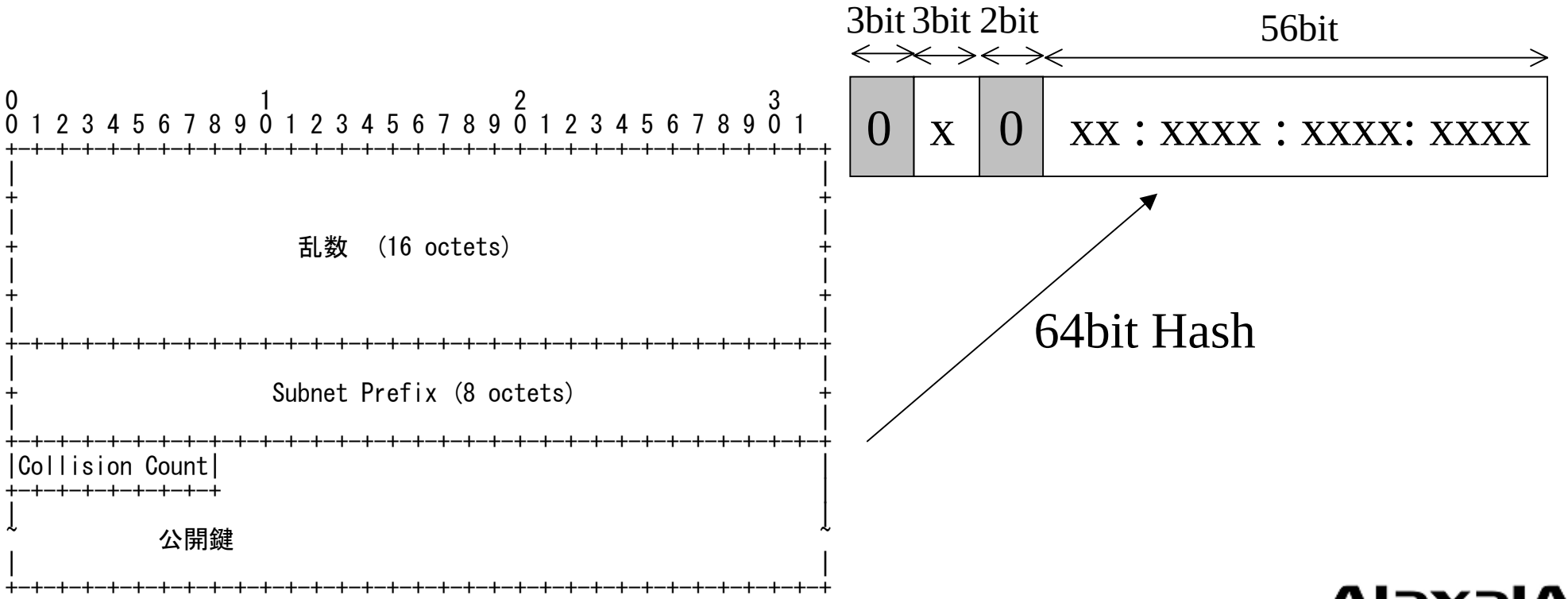
SSLと同様に、予め端末・ルータが「信頼できる公開鍵へのサイン主」を知っているのが大前提



IPv6仕様の現状（セキュリティ関連　---CGA---）

- IPv6リンクローカルアドレスを、SENDで用いる公開鍵から作成
- SENDと同時に使用することが多い

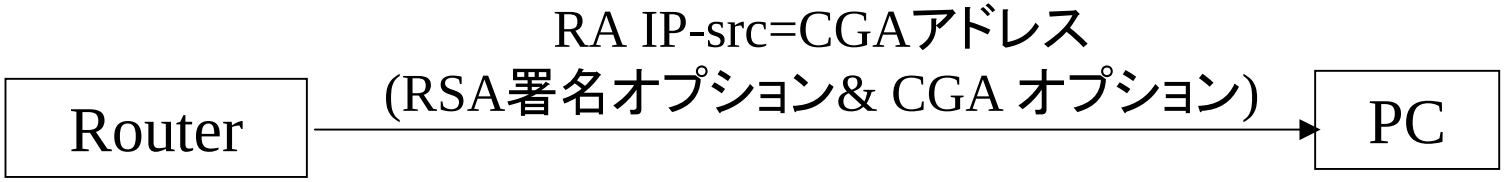




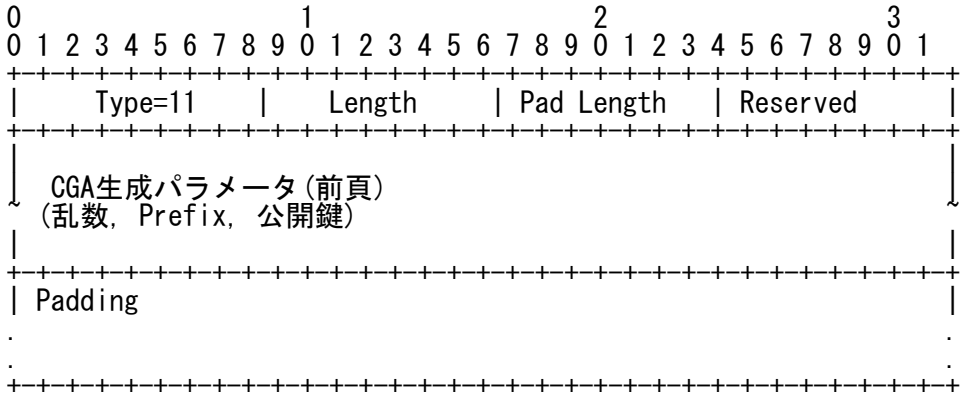
IPv6仕様の現状（セキュリティ関連　---SEND&CGA---）

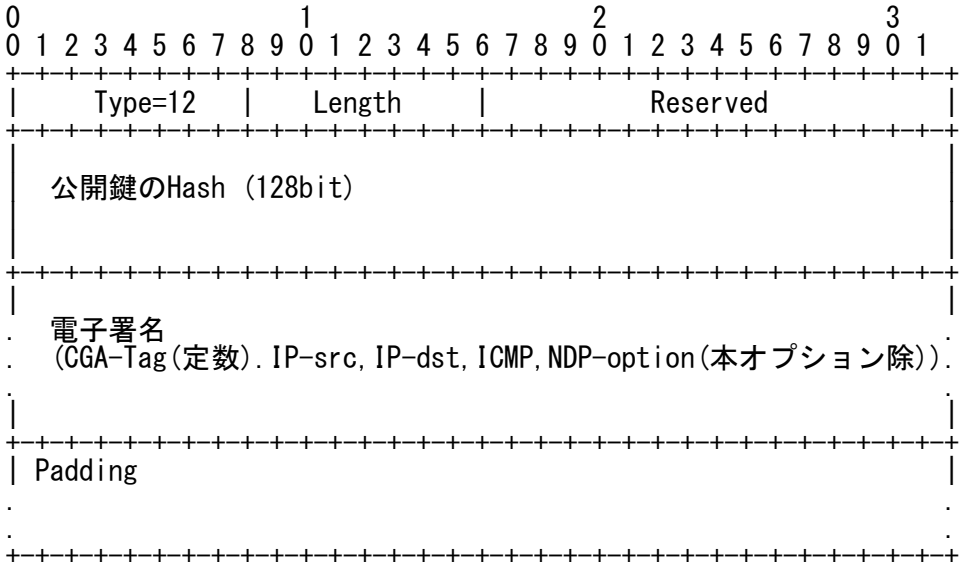
・NS/NA/RS/RAメッセージに自分の証明書で署名 & CGAアドレス生成元情報を添付

・受信者は、CPAで取得した公開鍵証明書と添付情報から、IP-srcやメッセージの正当性を確認



IP-srcとCGAオプションの整合性を確認
RSA署名とRouterの証明書の整合性を確認





IPv6仕様の現状（セキュリティ関連　---SEND&CGA---）

SEND&CGAの課題

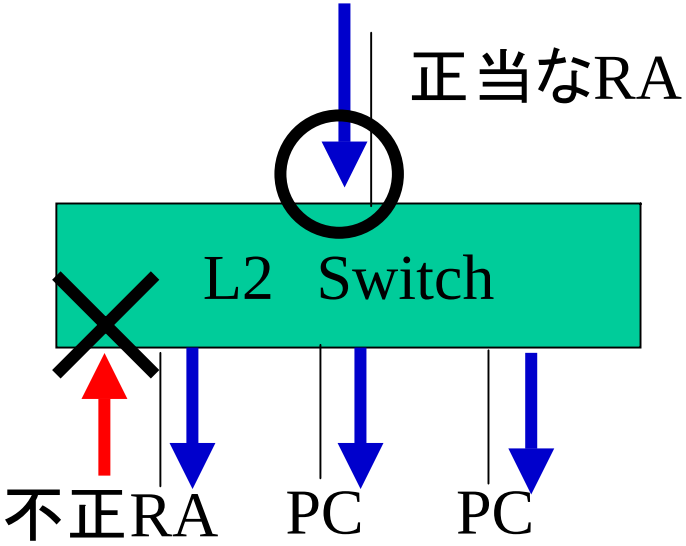
・まだあまり普及していない
　→結局SEND&CGA offなルータ・端末を信用せざるを得ない

・全端末・ルータにクライアント証明書を持たせる必要あり
　→普及が困難

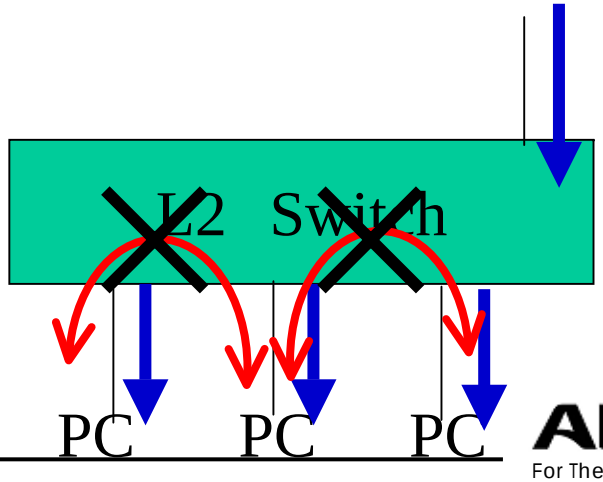
・結局「真っ当な証明書を有すること」しか確認できない
　→証明書取得済の端末から異常なNS/NA/RS/RAが流れてきた場合は、防ぎようがない

IPv6仕様の現状（セキュリティ関連　---RA Guard---）

・L2スイッチで、「正しくないRA」を廃棄
・「正しいRA」の定義は実装依存
　e.g.)
　・特定ポートから流れてきたRA
　・装置起動後5[s]以内に流れてきたRA
　…



※NS/NAやIPv4については別途対策が必要（e.g. DHCP-snooping）
→プロトコル非依存にL2レベルで対策する(e.g. Private-VLAN)のも効果的



IPv6仕様の現状（セキュリティ関連　---ICMPv6フィルタリングガイドライン---）

ICMPv6パケットをフィルタすると、IPv6通信自体が出来なくなることがある
（e.g. path MTU discovery失敗）
だからといって、ICMPv6パケットを無制限に通すのは怖い

	廃棄不可	通常は廃棄不可	Don't Care	管理者のポリシー次第	通常廃棄可
中継		MIP6	NDP, MLD, SEND, MR-disc.	Seamoby	NI-Query/Reply, Router Renum.
共通	Dst Unreach(全code) Packet-Too-Big Time-Exceed (code0) Param.Prob. (code1,2) Echo-Request Echo-Reply	Time-Exceed. (code 1) Param.Prob. (code0)		未割当ICMPv6エラータイプ （Type5-99, 102-126）	試験割当ICMPv6タイプ （Type100-101, 200-1） 未割当ICMPv6情報タイプ （Type159-254）
自分宛	NDP, MLD, SEND, MR-disc		Router Renum., MIP6, Seamoby	Redirect, NI-Query/Reply	

IPv6仕様の現状（セキュリティ関連　---IPv6でのアドレススキャン---）

・IPv4と比べて、1つのサブネットを単純にスキャンするのは大変
　IPv4=2^8, IPv6=2^64

・ただし、IPv6アドレスの特質を用いると、もっと楽にスキャンできてしまう
　e.g.）
　64bitのうち、24bitはMACアドレスのVendor部
　64bitのうち、真ん中の16bit (ff:fe) は実質固定
　=> 2^24までは絞り込める

[対策]
　・匿名アドレス (e.g. Windows-XP/Vista, FreeBSD, Linux, ...)
　・匿名アドレスでないアドレスについても、下位64bitにMACアドレスをそのまま埋め込まない (e.g. Windows-Vista)
　・CGA

IPv6仕様の現状（無線/モビリティ関連）

IPv6 over 無線の標準化が行われてきた

IPv6 over IEEE802.16　(RFC5121, 5154)

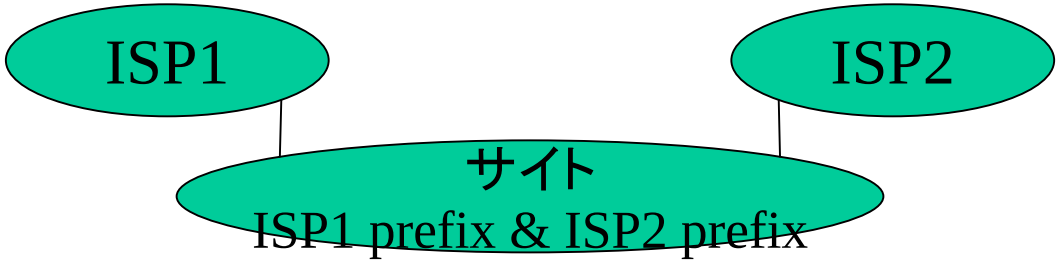
IPv6 over IEEE802.15.4　(RFC4919, 4944)

その他Mobile-IPv6関連の
標準化が多数行われている。

RFC番号	タイトル
4584	Mobile-IPv6向けソケットAPI拡張
4621	IKEv2 Mobility and Multihoming
4640	Mobile-IPv6 Bootstrappingの課題
4651	Mobile-IPv6経路最適化の分類と分析
4877	IKEv2・IPsec(改訂版)を用いたMobile-IPv6
4866	Mobile-IPv6経路最適化のエンハンス
4882	Mobile-IPv6におけるIPアドレスの場所のプライバシー
5026	Mobile-IPv6　Bootstrapping
5094	Mobile-IPv6ベンダー固有オプション
5095	Mobile-IPv6の実験的メッセージ
5142	Mobilityヘッダのホームエージェント切替メッセージ
5149	Mobile-IPv6におけるサービス選択
5268	Mobile-IPv6高速ハンドオーバ
5270	IEEE802.16eでのMobile-IPv6高速ハンドオーバ
5271	3G CDMAでのMobile-IPv6高速ハンドオーバ

IPv6仕様の現状（マルチホーム関連）

冗長性確保のため、複数のISPと接続
通常エンドユーザに付与されるのは、PA(Provider-Aggregable)アドレス
　→複数ISPと接続すると、端末には複数のIPv6アドレスが付与される
　アドレス選択の結果によっては、通信が成り立たないことがある。



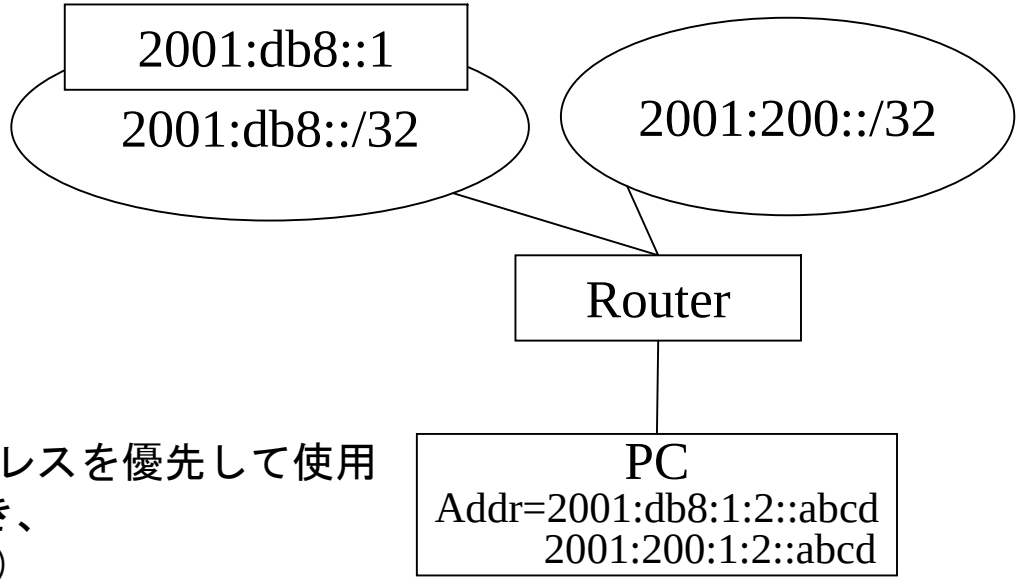
アプローチ

1. 端末に複数のIPv6アドレスを持たせない
　　マルチホームする場合には、PI(Provider Independent)アドレスを配布
　　(= 今のIPv4マルチホームと同様)
　　- IPv6の売りだった「PAアドレスによる経路集約効果」はなくなる。
　　- 1ブロックの大きさがIPv4よりも大きい分、経路エントリ数インパクトは少ない(?)
2. 端末が複数のIPv6アドレスを上手に使い分ける
　　ソースアドレス選択ルールを端末へ配布
　　SHIM6

IPv6仕様の現状（マルチホーム関連 ---ソース選択ルール配布---）

ソース選択ルール(RFC3484)にて規定されている、ポリシーテーブルを活用

Prefix	Precedence	Label
::1/128	50	0
2001:db8::/32	45	10
::/0	40	1
2002::/16	30	2
::/96	20	3
::ffff:0:0/96	10	4



※宛先と同じLabel値を有するソースアドレスを優先して使用
e.g.　端末が以下の2アドレスを有するとき、
　　2001:db8:1:2::abcd （Label=10）
　　2001:200:1:2::abcd （Label=1）
2001:db8::1へパケットを投げる場合は、2001:db8:1:2::abcdを使用

同ポリシーテーブルを、何らかのプロトコル(e.g. DHCP)で外から配布
**　単純なケースには対応できるが、複雑なケースには対応不能**

RFC5220,5221にて分析

IPv6仕様の現状（マルチホーム関連 ---SHIM6---）

端末に振られたアドレスを2種類に分類

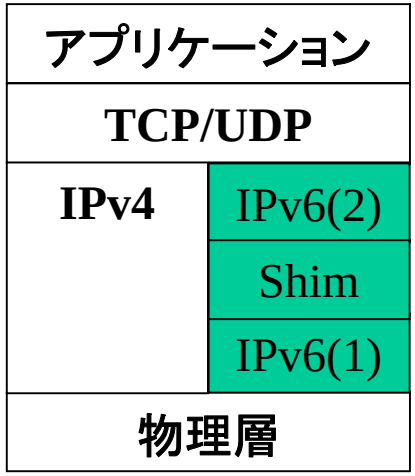
- Identifierアドレス　　端末の一意性を示すアドレス
- Locatorアドレス　　ルーティングするための場所を示すアドレス

IPv6層の間にShim層を導入

- Shim層の上からは、Identifierアドレスで通信しているように見える
- Shim層の下からは、Locatorアドレスで通信しているように見える

本質的には端末内NAT

- アプリケーションからNATを隠蔽し、端末外NATの抱える問題を回避



IPv6(2) = IP end-point sub-layer
- IPsec, Fragment, Destination Option処理

Shim
- Locator/Identifier対応付け
- Locator/IdentifierのIPv6アドレス付替

IPv6(1) = IP routing sub-layer
- NDP, IPv6パケット送受信処理

ISP1/2の両方からアドレス取得
src/dstにより、用いられるISPが決める

IPv6仕様の現状（マルチホーム関連 ---SHIM6---）

一見Mobile-IPv6に似ているが…
- Identifier(Mobile-IPv6ではHome Address)への到達性がなくなる事態も考慮
- アプリケーション単位に経路選択可能

到達性がなくなったら、どのような処理をすべきか
- 「到達性がなくなった」という判断基準は?
- Identifierの付替は必要?

Locator選択アルゴリズムはどうあるべきか
- 到達性だけで評価して本当によいのか?

現実のマルチホーミング運用との整合性
- 端末がマルチホームポリシーを決める設計→ネットワーク管理者は、端末に対してマルチホームポリシーを強要しにくい

IPv6仕様の現状（まとめ）

・基本仕様は固まった

・拡張仕様(特に、セキュリティ・マルチホーム)は、プロトコル標準化活動と現実の運用にギャップがある

IPv6運用の現状

・各種プロトコルのIPv6対応
　仕様はほぼ対応済

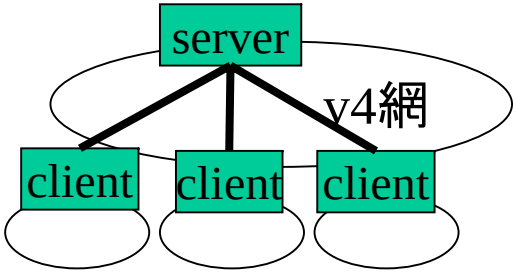
・各種運用ガイドライン
　前述のセキュリティ関連部にて説明済

・IPv6移行技術の議論
　後述

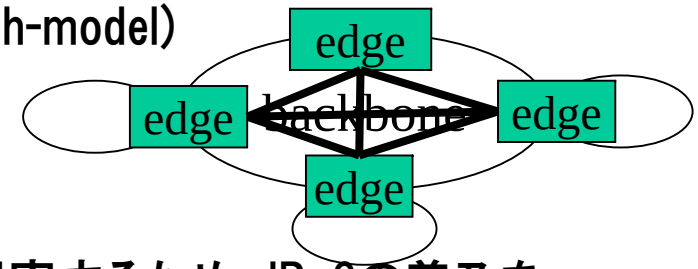
IPv6運用の現状（IPv6移行技術の議論）

・以下の3種類の議論を行っている
  a)IPv4しかないエンドユーザに対して、IPv6コネクティビティを提供する場合
  b)IPv4しかないバックボーン網で、IPv6コネクティビティを提供する場合
  c)IPv4アドレスが枯渇したときに、IPv6で何とかする場合

・現状は以下の通り
  a) L2TPv3トンネルでIPv6提供（Softwire hub&spoke-model）
    6to4/Teredo/ISATAPなどの自動トンネル



  b) コア網内でトンネルを自動的に張る。(6PE, Softwire mesh-model)



  c) 議論中
    NAT-PTは、「IPv6のメリットであるEnd-to-End通信を阻害するため、IPv6の普及を阻害する」と判断され、一度廃止された。(RFC4966)
    一方今日まで代替プロトコルが出てきていない
    →IPv4アドレスが枯渇する2011年までに議論が収束し、実装が提供されるか???

IPv6運用の現状 (IPv6移行技術の議論)

RFC5211 インターネット移行計画

IPv4アドレス枯渇を見越した、大雑把な移行時期の目安を提示

		準備段階 ～2009/12	移行段階 2010/1～2011/12	移行後段階 2012/1～
インターネットのIPv6化	コネクティビティ	試行サービス(SHOULD) (tunnelかnative)	商用サービス(MUST) (なるべくnative)	商用サービス(MUST) (native) (SHOULD)
	サーバ (e.g. Web, メール, DNS)	IPv6のみ版 (SHOULD) (dual-stack化はまだ)	IPv6版 (MUST) (商用レベル(SHOULD) dual-stackか否かは不問)	
イントラネットのIPv6化	コネクティビティ	-	試行サービス(SHOULD) (tunnelかnative)	試行サービス(SHOULD) (なるべくnative)
	サーバ (e.g.DNS,DHCP)	-	IPv6版(SHOULD)	

IPv6実装の現状

・装置の対応状況
・アプリケーションの対応状況
・システム/サービスの対応状況

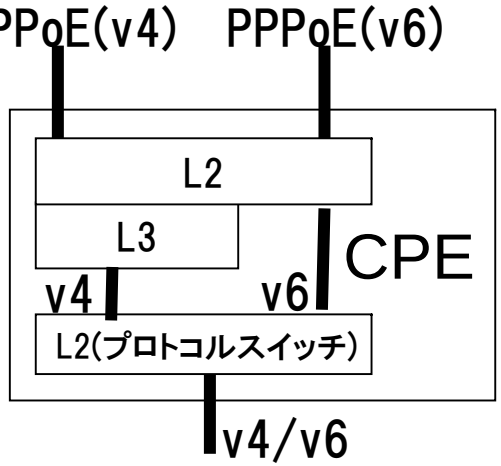
IPv6実装の現状（装置の対応状況）

・端末/サーバのOS
・バックボーン系のルータ/スイッチ
・アクセス系のBRAS/CPE
・サービス側の負荷分散装置など

IPv6実装の現状（装置の対応状況）

・端末/サーバのOSやバックボーン系の装置(ルータ/スイッチ/BRAS)
　最新のものはほぼ対応済
　　OS: Windows-XP/Vista/CE, Mac OS-X, BSD, Linux, Solaris, …
　　Router/Switch: Cisco, Juniper, ALAXALA, …
　　BRAS: Juniper, 日立, NEC, …

・アクセス系のCPE
　IPv6パススルーモードが大半
　IPv6 L3対応製品は稀
　　費用対効果が弱いことが本質的原因



・サービス側の負荷分散装置など
　IPv6にも対応している商品もある
　IPv4並のきめ細かい制御は難しいことが多い（次ページ）
　　IPアドレス長が長いことが本質的原因

IPv6実装の現状（装置の対応状況 –IPv4並のきめ細かい制御の難しさ--）

経路表や振分テーブルなどはCAM(Contents-Addressable-Memory)で実装されることが多い

パケットの内容自体をキーにして、テーブル検索

何エントリあっても、1Clockでマッチング可能

Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	その他…	Action

CAMで1Clockにマッチできるbit幅には上限がある（デバイス限界）

「きめ細かい制御」には、特に「その他」の部分の余りフィールドを用いることが多い

→IPアドレス幅が広がると「その他」フィールドの幅が狭まるため、IPv6ではきめ細かい制御が出来ないことがある。

CAMを複数用いてbit幅を増やすと最低でも2Clock分は必要→転送性能劣化

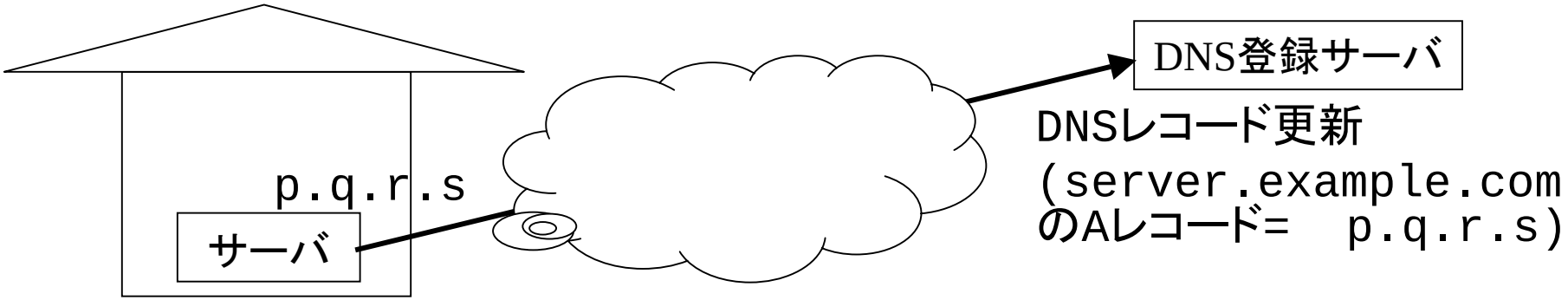
IPv6実装の現状（アプリケーションの対応状況）

	サーバ	クライアント			課題
		Win	Mac	Unix	
基盤アプリ (DNS/NTP)	△	△	○	○	Windows-XPはIPv6経由でのDNS検索不可 Windows-XPはIPv6経由でのNTP同期不可 レジストラがIPv6アドレス登録に対応していないことも多い
典型的アプリ (Web)	△	○	○	○	一部のブラウザではデフォルトでIPv6 disable アクセス解析のIPv6対応はまだ（DNS逆引きによる判断ができない）
典型的アプリ (メール)	△	△	△	○	IPv6対応クライアントは少ない サーバの拡張機能(ロードバランサ, Spam・Virus対策)はv6未対応なことが多い

IPv6実装の現状（アプリケーションの対応状況　---DNS---）

例. 簡易型Dynamic DNSサービス

あるURLにログインすると、そのアクセスに用いたIPアドレスをホスト名として登録



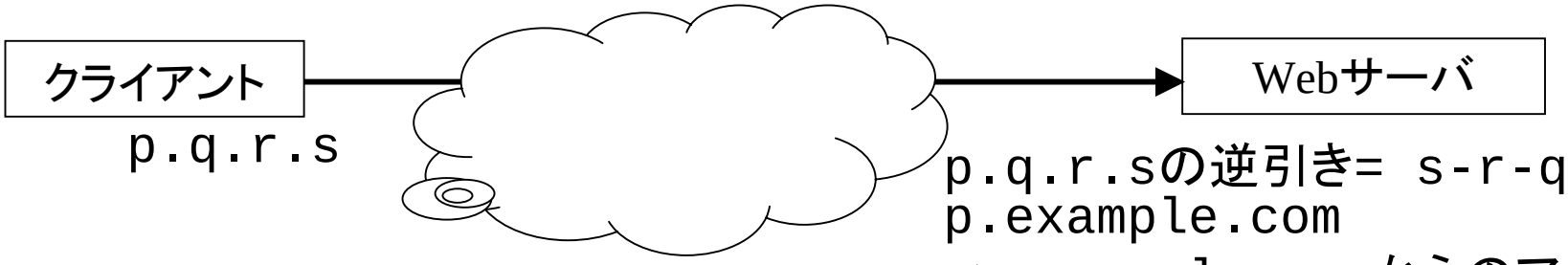
課題

1. IPv6 Connectivityが無いときには、IPv6アドレスを登録不可
2. IPv6 Connectivityがあったとしても、IPv4かIPv6アドレスの片方しか登録できない

複数種類のアドレスを持つことが本質的原因

IPv6実装の現状（アプリケーションの対応状況 ---アクセス解析---）

例. あるURLへのアクセスに用いたIPアドレスの持ち主を、DNS逆引きで算出



課題

- IPv6アドレスの逆引き登録は原理上困難

=> whoisなど、別データベースを参照する必要有

IPアドレス長が長いことが本質的原因

IPv6実装の現状（システム/サービスの対応状況）

- IPv6を使っているシステム/サービス

  新システム/サービスで最初からv6を使っている事例が多い

  - Flets.net
  - Flets光ネクスト (NGN)
  - Google （http://ipv6.google.com/）
  - IP電話
  - マルチキャストストリーミング (4th Media, 地震速報システム, 講義中継)
  - 2ちゃんねる over IPv6 (http://ipv6.2ch.net/)

- IPv6を禁止しているシステム/サービス

  DNSレコードを細工するWeb認証サービスで、IPv6を有効にした端末を接続できないことがあった(AAAA recordを扱えないため)

  WIDE v6fix WGにて解析

まとめ

・基本仕様はほぼ固まったが、拡張仕様についてはプロトコル標準化と現実の間にギャップがある

・IPv4->IPv6移行技術が普及しきる前に、IPv4アドレスが枯渇する可能性がある

・以下の2つの理由から、実装/サービスのIPv6化が遅れている
  ・技術的な難しさ（IPアドレスが長いこと、端末が複数のアドレスを持つこと）
  ・ビジネス的な難しさ（費用対効果）

2011年前後にはIPv4アドレスが枯渇すると言われている中、こうしたギャップをどう埋めるべきか?