2005 年 IPv6 移行ガイドライン

IPv6 設計運用に関する Tips

2005 年 3 月

IPv6 普及･高度化推進協議会

移行 WG

目次

ネットワーク管理

アドレス管理データベース

事業者の各種管理データベースにおける IPv6 対応状況

IPv6 アドレス管理方法でよいものはないかというのは、ISP や IDC などの運用側共通の課題となっています。これは、基本的に事業者依存の話で、規模が小さければ、Excel などで強引に対応できますが、規模が大きな場合は、RDBMS を駆使していかないと破綻します。

各種管理 DB は、現状でもパッケージ商品があるわけでもなく、各事業者でカスタマイズして作っている状況で、 IPv6 全盛期になっても状況は変わらず、汎用的なパッケージ商品はなかなか出ないのではないかと考えられます。したがって、RDBMS の IPv6 対応状況調査も必要ではないかと思われます。

IPv6 普及･高度化推進協議会では、IPv6 アドレス管理ツールを公開しています。

http://www.v6nic.jp/system/index.html

管理ツールの IPv6 対応状況

オープンソース系

オープンソース系の管理ツールでは、以下が IPv6 対応しています。

Nagios (http://www.nagios.org/)

ping6、ポート監視 (nagios-plugins-1.4.0alpha1)

Argus (http://argus.tcp4me.com/)

ping6、ポート監視

AS Path Tree (http://carmen.ipv6.tilab.com/ipv6/tools/ASpath-tree/)

BGP4+用管理ツール(BGP4+のルーティングテーブルを元にトポロジーを表示)

MRTG (SNMP over IPv6)

net-snmp (SNMP over IPv6)

それなりに使えるものがそろってきている状況です。

商用系

商用系では、次の製品が IPv6 対応しています。

HP OpenView

Eden

Ciscoworks (対応予定)

IPv4/IPv6 トランスレーション機能を使った監視

この他、既存の IPv4 **監視ツールをトランスレーション機能により** IPv6 **対応にする方法もあります。**

IPv6 Management Gateway

http://www.ipv6.man.poznan.pl/index.php?id=18

ICMP、TCP、SNMP **の** IPv6/IPv4 **トランスレーション**

横河電機 TTB **など**

http://www.yokogawa.co.jp/ipnet/ttb/

TCP、UDP、ICMP **の** IPv6/IPv4 **トランスレーション**

参考 URL

http://6nettools.dante.net/cgi-bin/moin/moin.cgi/WortIndex

http://tools.6net.org/toolsList/

http://www.idg.co.jp/nw/service/service.html

ネットワーク設計

ルータ、通信機器のアドレッシング

ルータ、サーバのアドレスは手動設定することをお勧めします。EUI-64 の利用によるアドレス自動構成では、NIC が変わるとアドレスも変わってしまうためです。

また、DNS 登録、フィルタリング設定の手間軽減のために、分かりやすいネーミングルールを考える手もあります。

::1、::53、::80、::cafe など、0〜9、a〜f を自由に組み合わせてポート番号や名前を表現
:c726:a00:3:82 で東京 03-広島 082 間の ATM リンクを表現するなど

ただし、こうした分かりやすいアドレスは攻撃対象になりやすいことも考慮したほうがよいと思われます。

リナンバリング方法

同一インタフェースに複数の IPv6 アドレスが付与可能であることを利用して、新旧アドレスを共存させる過程を経たリナンバリングが可能です。

手順としては、まず新アドレスを取得、次に新アドレスで接続性(ルーティング)設定を行います。そして IPv6 ノード(ルータ及び端末)へ新アドレスを付与します。この際、旧アドレスも削除せずに付与しておきます。端末レベルではアドレス自動構成を使います。これと併せて、DNS 登録変更作業等を行います。次に、旧アドレスを削除し、旧アドレス接続性(ルーティング)を削除します。

上記の手順により、IPv4 のリナンバと比べ、サービス断の影響が少なく段階的なリナンバが可能となります。

次のインターネットドラフトがあります。

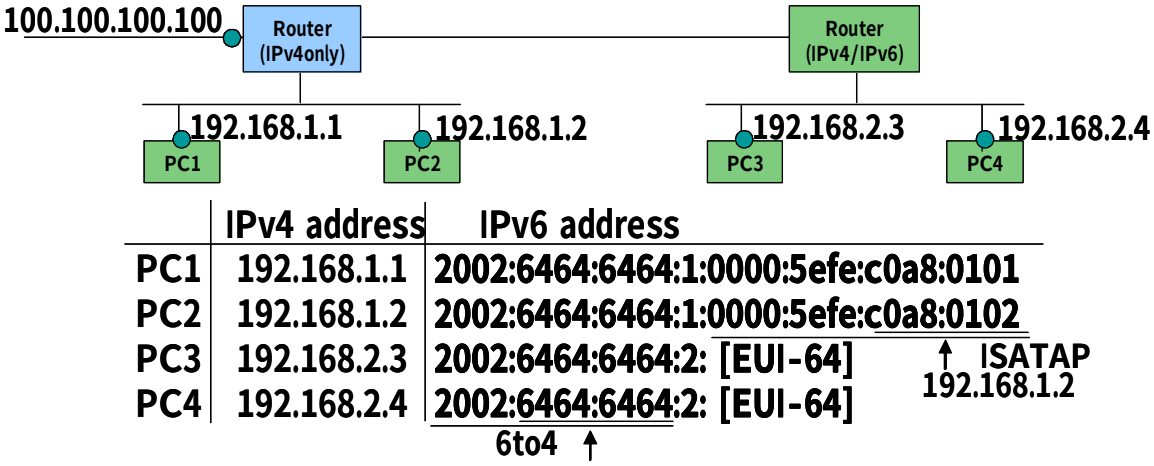
Procedures for Renumbering an IPv6 Network without a Flag Day
(Draft-ietf-v6ops-renumbering-procedure-01.txt)

企業内 IPv6 ローカルアドレス付与方法

IPv6 において、プライベートネットワークにおける利用を想定したアドレスとして考えられていた“サイトローカルアドレス”は、使用されないことが正式に決定しました。それでは、閉域ネットワークで IPv6 を実験的に導入する場合の IPv6 アドレスは、どのように付与すればよいでしょうか。

(1) グローバル IPv4 アドレスと 6to4 アドレス生成ルールを利用

これは、対象ネットワークが将来インターネット接続された際、正式な IPv6 アドレス取得後、IPv6 ローカルアドレス設定情報が残存した場合でも、アドレス重複が発生しないことを考慮したものです。6to4 では、ネットワークプレフィックスとして、2002::と 6to4 リレールータの IPv4 アドレスを 16 進表現したものを組み合わせて利用します。下の図のように、ルータの IPv4 アドレスを使い、6to4 のルールに基づいたアドレッシングの下で、組織内の IPv4/IPv6 デュアルスタック端末間の通信を実現することができます。



2) グローバルユニーク･ローカルアドレス (fc00::/8, fd00::/8)

グローバルユニーク･ローカルアドレスは、サイトローカルアドレスの代替として、世界に 1 つしかないプライベートネットワーク用のアドレスを割り当てるものです。ただし、現在 IETF で議論が始まったばかりで、まだ利用を推奨することはできません。

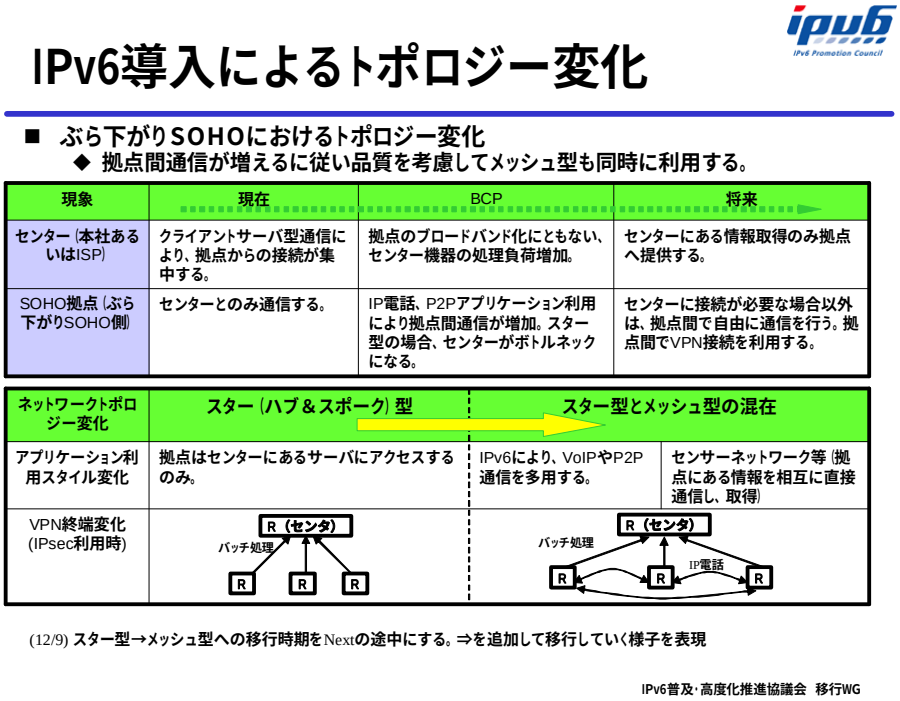
ぶら下がり SOHO のネットワークトポロジー

ぶら下がり SOHO と本社との通信形態は、IPv6 導入の進展とともに変化していくことが考えられます。

IPv6 移行にともない、全通信を IP 網に頼る SOHO において、従来のクライアントサーバ型のアプリケーションだけでなく IP 電話のような P2P アプリケーションの利用増加も考えられます。

P2P アプリケーションを利用する際は、従来のスター型接続では一箇所に通信が集中してしまい、品質劣化の危険性があります。

拠点間との P2P 接続が可能なメッシュ型接続が必要となるため、同時にスター型とメッシュ型が利用できる接続形態が求められます。



企業のマルチホーミング

企業におけるマルチホーミングの目的は、SOHO では用途別の回線使い分け（SNA 系は専用線、Web やメールは ADSL 回線を利用する、など）、バックアップ通信路の確保（候補としては ADSL、ISDN など）が主な目的となります。その他に、負荷分散やパフォーマンスの最適化が目的となります。

こうした目的ごとにマルチホーミングの要件をまとめると、以下のようになります。

用途別の回線使い分け

この場合、用途（アプリケーション）で異なる回線を選べることが要件です。プルでもプッシュでも、同一のアプリケーションなら行きと帰りで同じ回線を利用します。

バックアップ通信路の確保

ある回線が利用できなくなったら他の回線を使うという利用法です。 したがってメイン回線が使えるときは他の回線を通さない（双方向とも） ようにしなければなりません。回線切り替え時にセッションが切れないことも必要です。

マルチホーミング技術・手法（outbound）

outbound のマルチホーミングには、以下のような手法があります。

端末ごとに異なるゲートウェイを設定

これは端末単位で使う回線を分ける方法です。

端末が振り分ける

その 1 つは、端末自体が宛先アドレスで振り分ける方法です。この場合、端末はデフォルトゲートウェイ以外の経路も持つことになります。

もう 1 つは、端末でポリシールーティングを実施する（アプリケーションで振り分ける）方法です。

ゲートウェイ（ルータ、負荷分散装置）が振り分ける

これには、宛先アドレスで振り分ける方法、ポリシールーティング（アプリケーション、送信元アドレスによる振り分け）、ECMP などランダム的負荷分散があります。

内向き DNS

これは、用途（FQDN）で答えるアドレスを変える（ぶらさがり SOHO）というものです。バックアップや負荷分散目的で、複数アドレスを設定できます。

VRRP、HSRP、ESRP など

バックアップ目的で利用されるネットワーク機器の冗長性確保のためのプロトコルです。回線落ちの際に、ルータ擬似ダウンのような拡張機能が実装されたルータもあります。

マルチホーミング技術・手法（inbound）

inbound のマルチホーミングには、以下のような手法があります。

BGP

これは経路が増えるので、大規模なネットワークの場合しか許されません。

個別的 ISP 対応

ISP 間でローカルに経路を流し合うなどが考えられます。

ネットワークの途中でアドレスを変更する技術

これには NAT、プロキシ、トンネリングが考えられます。

外向き DNS

これは用途（FQDN）で答えるアドレスを変えるものです。バックアップや負荷分散目的で、複数アドレスを設定することができます。

マルチプレフィックス

同一リンク（インタフェース）で複数のプレフィックスを設定するものです。IPv6 では複数アドレス前提なので広く使えます。プル型のアプリケーションでは、用途に応じて端末がソースアドレスを選択することが可能です。

Mobile IP

モバイルでない端末にも、あえて Mobile IP を適用し、気付アドレス（care-of address）を使い分けるという方法があります。

IPv6 のマルチホーミング

SOHO に関しては、IPv4 におけるマルチホーホーミングの手法として利用できるのは、現状では NAT しかありません。

なぜなら、SOHO で AS をもらうのは無理ですし、punching hole は問題視されています。同一端末に複数アドレスを設定することも一般的ではありません。そもそもマルチホーミングなくても NAT しているという事情もあります。

しかし、これには P2P アプリケーションの利用が困難という問題があります。

一方、IPv6 ではマルチプレフィックスが手段として有効と考えられます。RFC3178（secondary link を使う）の方法はコスト高です。

特にぶらさがり SOHO ではサービス毎にアドレスを分けることでうまく運用できそうです。プル型アプリでは source address selection の機能が重要となります。

マルチプレフィックスの利用に関しては、IETF の multi6 WG で検討中で、その目的だけは RFC 化済み（RFC3582）となっています。

IPv6 の source address selection

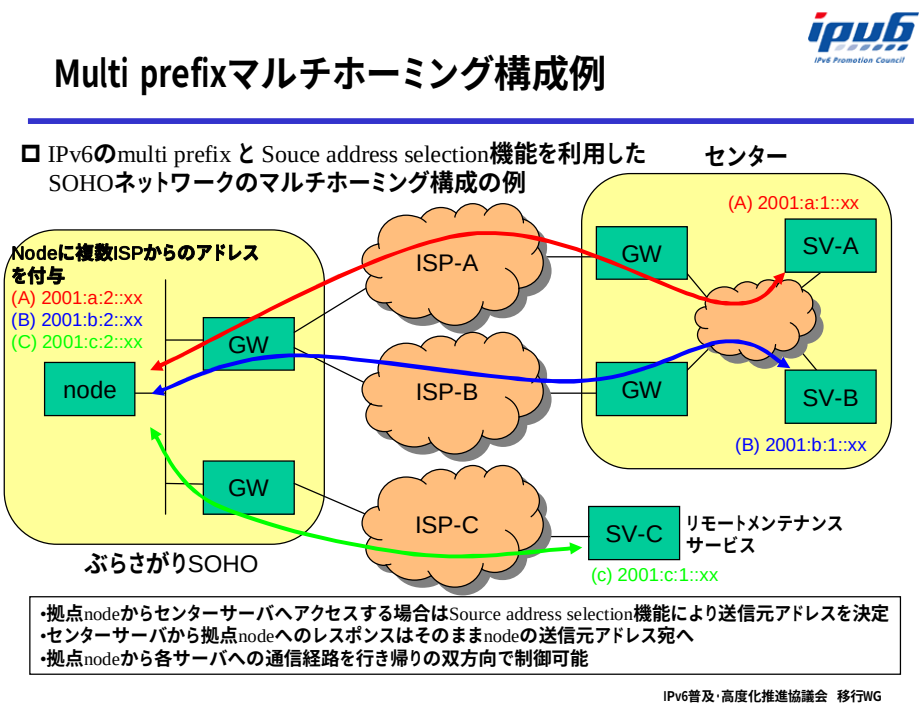
IPv6 における source address selection は、RFC3484 Default Address Selection for Internet Protocol version 6 (IPv6)として RFC 化されています。ここでは、source address を選ぶルールとして、以下の8つを定義しています。

1.destination と同じアドレスを優先
2.destination とスコープ的に近いアドレスを優先
3.deprecated でないアドレスを優先
4.care-of address より home address を優先
※ アプリで逆転できるメカニズムを提供するべき(SHOULD)
5.そのパケットを送信するインタフェースのアドレスを優先
6.policy table 上でラベルが destination と同じアドレスを優先
7.temporary address より public address を優先
※ アプリで逆転できるメカニズムを提供しなければならない(MUST)
8.destination と一致部分が長いアドレスを優先(longest match)

上記の 8 つのルールのうち、アプリケーションで使い分けるには、現状では 8.のルールが利用できます。ただし、計画的アドレス設計が必要となります。また、6.のルールは全端末に設定が必要な点が難点となっています。

マルチプレフィックス・マルチホーミングの構成例

下図では、ぶらさがり SOHO における単一の端末に、複数 ISP からのアドレスを割り当てており、この端末は、source address selection で送信元アドレスを選んで通信します。



マルチプレフィックス・マルチホーミングの課題

マルチプレフィックス・マルチホーミングには、主にデフォルトルータ選択と回線切り替えに関する課題があります。

デフォルトルータ選択

回線毎にデフォルトルータが分かれている場合、どれに送るか分からないという問題があります。RFC2461 (Neighbor Discovery)では特に基準が決められていません。

ルータがそのまま回線に転送してしまうと、用途が合わない可能性があるほか、ISP の ingress filter にひっかかる可能性があります。

対策としては、今後、端末の実装を改良し、source address を見て、対応する RA 送出元ルータに送る、draft-ietf-ipv6-router-selection-02.txt (RA で経路を流す拡張)のような仕組みを組み込むなどが考えられます。しかし、それまではとりあえずルータ側で redirect することで対応するしか方法はありません。

回線切り替え時の挙動

回線切り替え時に、即座にアドレスを切り替えられないと、別回線のアドレスで ingress filter にひっかかり、通信が途絶えることが考えられます。ルータで回線断を検出した場合、RA に反映で

きるといいのですが、End-End は別です。

　また、IPv4 において NAT を利用している場合でも同じですが、回線の切り替えに対応してアドレスが変わるのでは、セッションが切れてしまいます。たとえば Mobile IP など、セッションを維持するしくみが必要となります。

サーバシステム管理

企業内 DNS の設定方法

DNS サーバの設定

正引きの設定

IPv4

・A レコード

www IN A 1.2.3.4

IPv6

・AAAA レコード

www IN AAAA 2001:db8::80

・A6 レコードは使わない方がよい。

逆引きの設定

IPv4

・ in-addr.arpa ドメイン

4.3.2.1.in-addr.arpa IN PTR www.hogehoge.jp

IPv6 (→セキュリティガイドライン参照)

・ip6.arpa ドメイン

・ip6.int は過去の互換性のため、設定しておくとよい。

0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6
.arpa IN PTR www.hogehoge.jp

＜IPv6 アドレス登録の考え方＞

IPv4 アドレスが DNS 登録されている既存サービスについて、追加で IPv6 対応する際は、

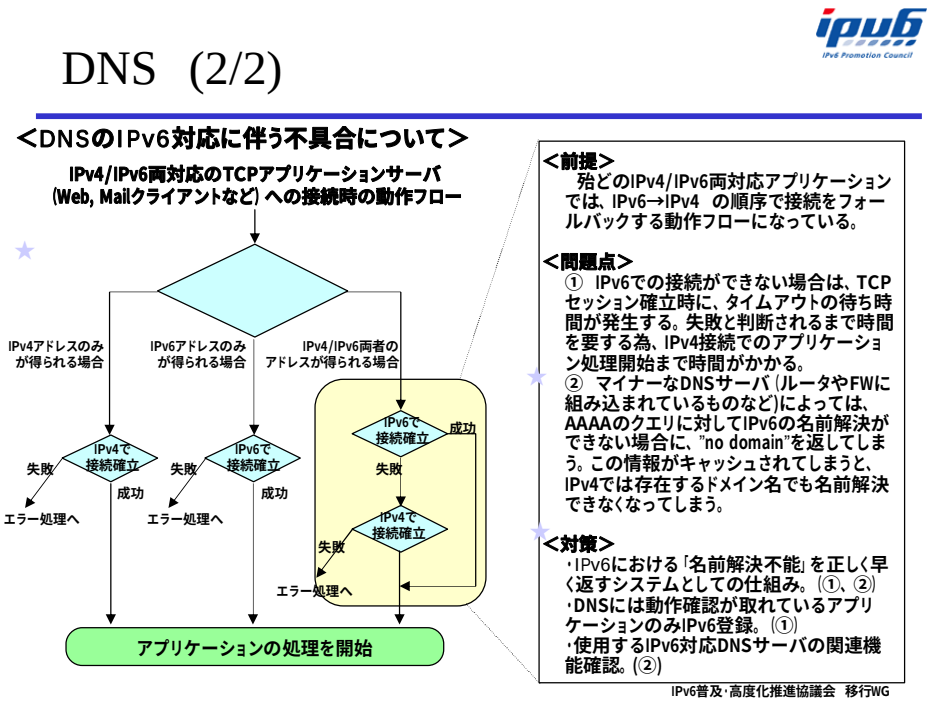
(1)A レコードと同一のドメイン名を、AAAA レコードでも登録する。

(2)A レコードとは別のドメイン名を、AAAA レコードで登録する。

の 2 通りが考えられる。通常、IPv4 から IPv6 へ移行する場合は、IPv4 と IPv6 でユーザがドメイン名を使い分ける必要がない(1)にした方がよいが、意図的に IPv4 サービスも継続する場合は、(2)の選択も考えられる。

DNS の IPv6 対応に伴う不具合について

IPv4/IPv6 対応アプリケーションでは、IPv6 → IPv4 の順序で接続をフォールバックするものがほとんどです。この問題点としては、IPv6 でのタイムアウトに時間を要するため、IPv4 での処理開始まで時間がかかります。また、DNS サーバによっては、IPv6 の名前解決ができない場合に、no domain を返してしまい、IPv4 での名前解決を妨げるものがあります。



情報家電の名前管理

ネーミング

ネーミングについては、家庭内の機器からの DNS サーバ発見、登録、名前解決の機能が必要となります。課題となるのは、DNS サーバの発見方法、クエリの送信方法、そしてトランスポートプロトコルの使い方です。

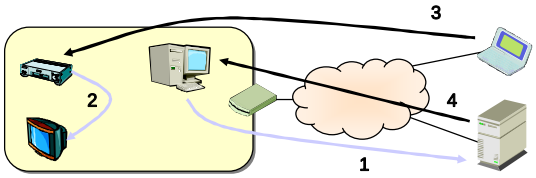
また、利用形態としては、誰が誰の名前を解決（正引き）できるようにするか（たとえば家庭外の任意の端末から家庭内の端末のアドレスが分かるようにすべきかどうか）を明確にする必要が出てきます。

ネーミング

- 機能的には・・・登録/解決、DNSサーバ発見、名前付け方法
- 方法的には・・・クエリの送信方法、DNSサーバの発見方法、トランスポートプロトコル

- 名前解決の目的による分類

	誰が	誰を解決する？
1	家庭内ノード	家庭外ノード
2	家庭内ノード	家庭内ノード
3	家庭外ノード（信頼関係あり）	家庭内ノード
4	家庭外ノード（信頼関係なし）	家庭内ノード



- ケース2はサービス発見と密接に関連する
- ケース3、4は家庭外ノードに対する情報提供方法とその安全性に対する議論が必要

家庭内での名前解決（ケース２）における課題

家庭内での名前解決（ケース2）：課題

- 家庭内ノードが家庭内ノードを解決したい場合、以下の検討事項がある

◆DNSサーバ発見プロセス
- ➢Multicast
- ➢Anycast
- ➢自動設定プロトコル
- ➢手動設定
- ➢サーバ不要方式

◆機器情報の登録
- ➢機器の名前
  - – DNSの枠組み
  - – DNS以外の枠組み
- ➢IPアドレス
- ➢その他の付加情報

◆クエリモデル
- ➢Multicast
- ➢Anycast
- ➢Unicast
- ➢ICMPv6 Node Information Query

◆ドメイン名
- ➢DNSの枠組みを利用する場合
  - – 家庭はどのドメインを使うべきか
    - » ISPから委譲される？
- ➢利用者が適当に命名？

家庭内での名前解決（ケース２）における対応案

DNS サーバ発見プロセス

DNS を利用するには、端末が DNS のアドレスを何らかの方法で知らなければなりません。しかし、家庭では、設定するインタフェースを持たない機器が存在するため、この情報を自動設定する必要があります。

自動設定の方法にはいくつかありますが、well-known のエニイキャストやマルチキャストを使う場合、セキュリティ問題への検討が必要となります。

IETF ドラフトでは、Router Advertisement、DHCP、well-known マルチキャストが列挙されています。

DNS サーバを利用しない方法が登場する可能性もあります。

家庭内での名前解決（ケース2）：対応案

- DNSサーバ発見プロセス
  - 設定するI/Fを持たない機器の存在 ⇒ 自動設定の必要性
  - Well known Anycast, Multicast使用により設定を省略可能
    - セキュリティへの検討が必要
  - IETFによる議論(draft-ietf-dnsop-ipv6-dns-configuration)
    - 次の3方式が列挙されており、1つには絞り込まれていない
    - 各方法に対する利点と欠点が整理されている
    - RA
    - DHCP
    - Well known multicast
- DNSサーバに依存しない別の方法が登場する可能性もある
  - non-PC主導によるIPv6の普及シナリオが描けた場合

IPv6普及・高度化推進協議会　移行WG

クエリモデル

マルチキャスト DNS の場合、個々のノードでの対応と外部問い合わせ用サーバが必要となります。ICMP Node Information Query (NIQ)は、そもそも DNS ではないのでプログラム修正が必要です。エニイキャスト DNS、マルチキャスト DNS では、セキュリティ面の問題があります。

家庭内での名前解決（ケース2）：対応案

- クエリモデル
  - Unicast
    - 既存DNSの通り
  - Anycast
    - 再帰問い合わせをサポートするサーバを利用することで、内外サーバを共用可能
    - AnycastアドレスはDHCPで配布してもよいし、Well Knownのアドレスを定義してもよい（現状未定義）
  - Multicast
    - 個々のノードがマルチキャストによる名前解決に対応する必要がある
    - 外部のDNSサーバを通じて名前解決をするためのサーバが必要
      - Multicast DNSの場合には、問い合わせは転送されないため
  - ICMPv6 Node Information Query
    - DNSではない
      - プログラムの修正が必要
        - » 問い合わせ側：レゾルバを改造し、OS上は通常の名前解決機構として利用できるようにする
        - » 応答側：Node Information Queryに対する対応が必要
  - Anycast、Multicast DNSに関するセキュリティの問題
    - プロトコル上、どのサーバが受信するか、どのサーバから応答が返ってくるか保障がない

機器情報の登録

PC であっても、IPv6 アドレスの登録は大変な作業ですし、家庭には表示や入力手段を持たない機器が存在することが考えられます。したがって、自動登録手段は必要です。

この場合、家庭内ではあっても、登録された情報をどの範囲で公開するのかを制御しなければなりません。使用する名前については、機種名を使うことも想定できますが、ある家庭内に同一機種が複数存在する場合、どう区別するかという問題が発生します。

家庭内での名前解決（ケース2）：対応案

- 機器情報の登録
  - IPv6アドレスをDNS（または相当手段）に登録する作業は困難
    - 表示装置、入力装置を持たない機器の存在
    - 5：5の世界では多数のノードが接続する可能性がある
    - ⇒ 自動登録手段は必要
      - 接続検出（アドレスの変更）と自動登録の連携
        - » DNS UPDATE、など
  - 物理的な位置との対応関係
    - ユーザに対する利便性を考慮すると『camera01』よりも『玄関のカメラ』という感覚でアクセスしたい
      - DNS上に登録する情報は『camera01』でも良いが、ユーザに見せるためには変換が必要
  - 問題点
    - どの範囲に公開するのか
      - プライバシーの扱い
    - 名前の付け方：同一機種が複数存在する場合どう区別するのか？

IPv6普及・高度化推進協議会　移行WG

家庭外からの名前解決（ケース３、４）　における課題

家庭外端末からの家庭内端末の名前解決（前出の「名前解決の目的による分類」の表ではケース 3 とケース 4 に相当）については、登録にダイナミック DNS や DNS アップデートの既存の仕組みを利用できますが、どこを登録先とするかが課題です。また、登録情報や登録対象機器について取り決める必要があります。プライバシー保護の観点から、情報の公開先や公開内容は非常に重要な問題です。

家庭外からの名前解決（ケース3，4）：課題

■ 家庭外ノードが家庭内ノードを解決したい場合

◆登録

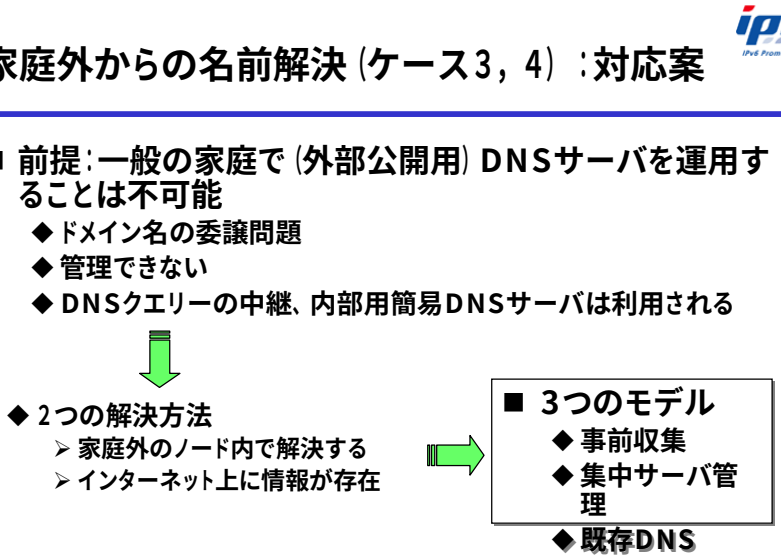
- DDNS，DNS update
- 登録先
  - ISP提供サーバ
  - 機器ベンダ提供サーバ
  - 第三者提供サーバ
- 登録情報
  - 登録情報･登録対象機器の決定
- 情報の公開先/公開内容
- プライバシーの確保

IPv6普及･高度化推進協議会　移行WG

家庭外からの名前解決（ケース３、４）における対応案

一般の家庭でDNSサーバは運用できません。したがって、端末内で解決するか、インターネット上に情報が存在するかのどちらかしかありえません。そこで、事前収集、集中サーバ管理、既存DNSの3つのモデルを用途で使い分けることになると思われます。

家庭外からの名前解決（ケース3，4）：対応案



事前収集モデル

事前収集モデルでは、家庭の内外を移動する機器が、家庭内にいる間に、たとえば/etc/hostsの情報を取得しておき、家庭外に持ち出された場合にこれを使って名前解決をすることが考えられます。この場合、情報は持ち出された機器の内部にのみ存在するので安全です。しかし、機器毎の設定は必要となります。また、設定後(持ち出し後）のアドレス変更には追従できません。

家庭外からの名前解決（ケース3，4）：対応案

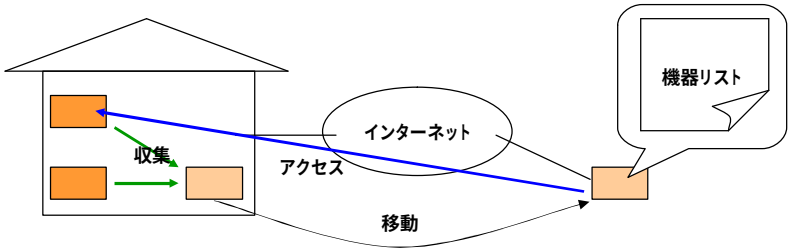
■ 事前収集モデル

◆たとえば/etc/hostsを持つ

◆情報はノードの内部にのみ存在するので安全

→ノード毎の設定は必要

◆設定後(持ち出し後）のアドレス変更には追従できない



IPv6普及・高度化推進協議会　移行WG

集中サーバ管理モデル

この場合、何らかの契約に基づいて、インターネット上に置かれたサーバで DNS 情報を管理します。この DNS サーバは、登録済みノードのみアクセス可能とします。登録は専用ソフトで行うことになるかもしれません。

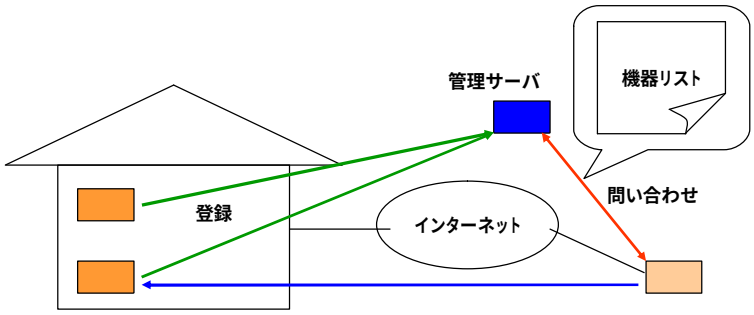
家庭外からの名前解決（ケース3，4）：対応案

■ 集中サーバ管理モデル

◆契約に基づくサーバで管理

◆登録済みノードのみアクセス可能

◆登録は専用ソフトで行う？



既存 DNS モデル

これは既存 DNS サーバに登録するもので、登録済みノードのみアクセス可能ですが、まず、登録方法の自動化をどうするかという問題（専用ソフトを利用する可能性）と、情報の公開範囲やプライバシー問題をどう処理するかという問題があります。

家庭外からの名前解決（ケース3，4）：対応案

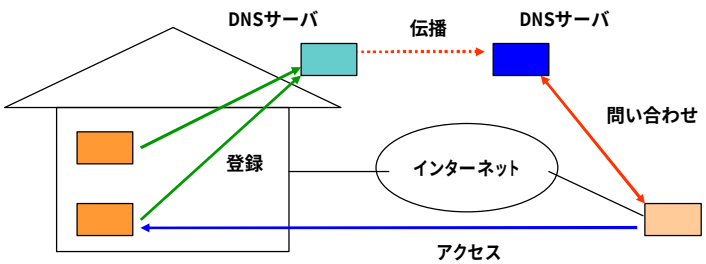
■ 既存DNSモデル

◆DNSサーバに登録

◆登録済みノードのみアクセス可能

◆登録方法（専用ソフトによる自動登録？）

◆情報の公開範囲・プライバシー問題



ネーミングに関するその他の課題

その他の課題の 1 つには、DNS 関連で利用するトランスポートプロトコルをどうするかという点があります。これについては、デュアルスタックが望まれます。理由は、IPv4 のみ、あるいは IPv6 のみで解決できる名前があってはならないということにあります。また、家庭用ルータへの搭載を考えるとデュアルスタックで問題はないと思われます。

もう 1 つの課題は、マルチプレフィックス／マルチホーム環境です。IPv6 では、1 台の端末に複数のネットワークプレフィックスが割り当てられる可能性があります。しかし、エンドノードでどのようにこれらを使い分けて、アプリケーションのためのソースアドレスを選択するかという点については、はっきりした解答が見出されていません。

また、DNS に関する通信のセキュリティ確保に向けて、DNSSEC が議論されていますが、まだ結論には至っていません。

ネーミング：その他の課題

- トランスポートプロトコルの選択
  ⇒やはりデュアルスタック
  - ◆サーバ側は広く対応していることが好ましい
    - ➢ルータ（家庭用）への搭載を考えるとデュアルスタックで問題はない
- マルチプレフィックス／マルチホーム環境
  - ◆IPv4ではPPPoEマルチセッションで実施
    - ➢DNSクエリを適切にルーティングする方法が実装されている
      - – 設定は静的に行う場合が多い
    - ➢NATがあるため、問題が顕在化しなかった
      - – エンドノードはマルチホームを気にする必要が無かった
  - ◆IPv6の場合、ソースアドレス選択が重要になる
    - ➢DNSで適切な応答を返さないと、ソースアドレス選択がうまく動作しない可能性がある
- DNSSEC

IPv6普及・高度化推進協議会　移行WG

また、Non PC 機器への自動的な名前付けについては、同一機種が複数あった場合、どうやって区別するのかという課題が残ります。また、アプリケーションで一覧表示した場合など、ユーザにとって分かりやすい名づけがほしいところです。このあたりまで含めた自動化が望まれます。

ネーミング：その他の課題（Cont.）

■ non-PCな機器への名前付け

◆同一機種が複数あった場合（TVやビデオ/DVD機が複数ある場合）どうやって区別するのか

◆アプリで一覧表示した場合など、ユーザにとってわかりやすい名づけが欲しい

- ➢ 家庭での配置と対応関係を持たせたい
  - – 玄関のカメラ
  - – リビングのエアコン　など

◆できれば自動化したい

利用モデル

遠隔監視・遠隔制御

機器監視・遠隔制御の需要

プリンタの遠隔サポート、PC 端末のソフトウェアメンテナンスなど、IT 管理のアウトソースに関する需要が存在します。特に SOHO は、こうした管理業務をアウトソースしなければならないケースが多く、アウトソースすることで管理レベルが向上するとも言えます。

そして、遠隔的な監視や制御には、LAN 内部の機器と外部の機器の通信が必要になります。

機器監視・遠隔制御の形態

遠隔監視や制御の形態には、プル型とプッシュ型があります。

プル型

これは、LAN 内部にある機器のみイニシエータになれるものです。従来のセキュリティの枠組みで実現しやすいという利点がありますが、通信に遅れが発生する、無駄に帯域を消費する、という欠点を伴います。

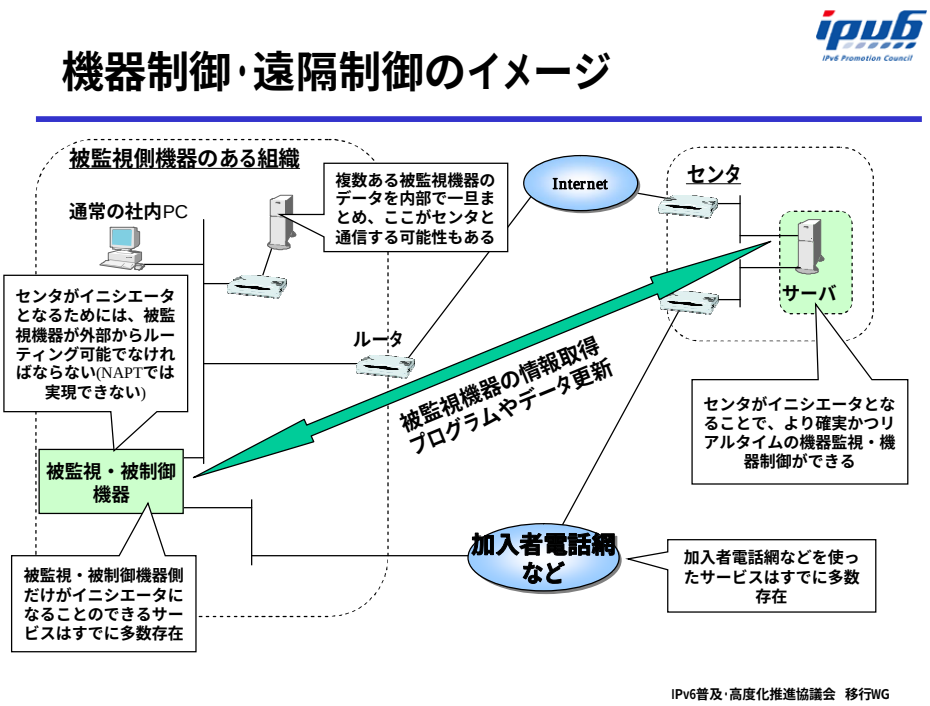
プッシュ型

LAN 内部の機器だけでなく、外部の機器もイニシエータになれる形態です。外部からのルーティング可能な IPv6 でこそ、実現可能性が高いと言えます。 これには、様々な新ビジネスの可能性があります。

機器制御・遠隔制御のイメージ

下は、遠隔監視や制御を図式化したものです。

まず、電話回線網などを使った遠隔監視･制御サービスは多数存在しています。さらに、インターネットを使った場合でも、プル型、つまり監視や制御の対象となる機器だけがイニシエータになるサービスは多数あります。管理センター側がイニシエータとなれば、確実かつリアルタイム性に優れたサービスを実現できます。



プル型の問題とプッシュ型の利点の例

プル型の欠点として、現在の Windows Update にも見られるように、対策が遅れることや、結局対策されないことがあるということが挙げられます。未だに Blaster や Nimda などがなくならないことは、これを如実に示しています。

では、Windows Update がプッシュ型だったらどうでしょうか。遅滞なく相手と通信し、センター側でアップデートされていないものを管理できるほか、アップデートできなかった環境にだけ、アップデート CD を無料送付するなどの対策も可能になります。

このように、リアルタイムのコントロールサービスを利用するなら、外部がイニシエータにならざるを得ません。サーバ管理のアウトソース(外部からサーバに telnet する)などがこれに当てはまります。

監視に利用するネットワーク

遠隔監視や遠隔制御には、さまざまなネットワークが利用されます。

非 IP 網(電話など)

価格が高いものの、IP による透過的な通信が行いにくいという問題があります。

専用線・広域イーサ網・IP-VPN 網など

大規模でないと費用対効果が低い、管理が面倒という特徴があります。

インターネット VPN 網

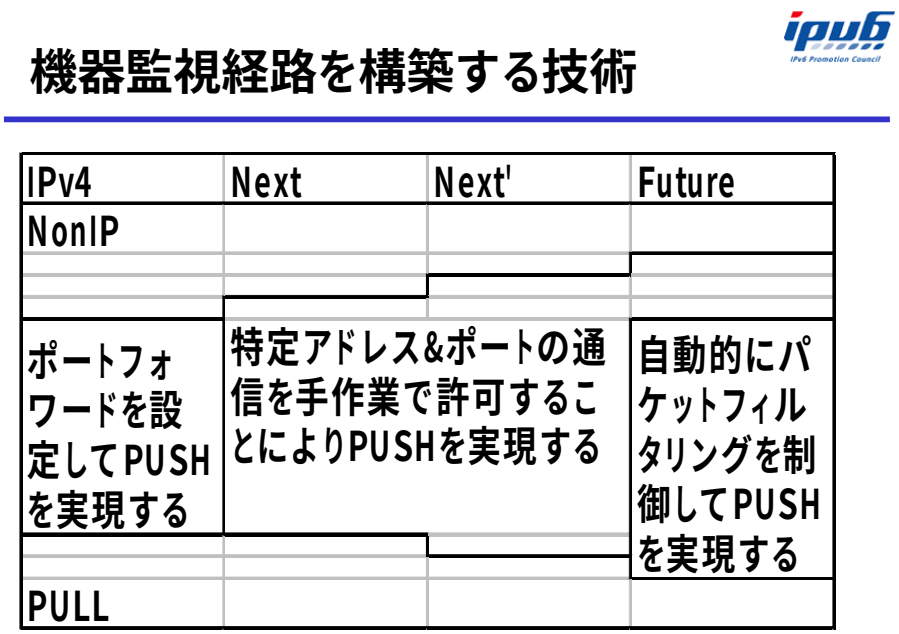
価格が安いですが、トンネリングの欠点があり、機器のコストが必要となります。

IPSec トランスポートモードによる監視通信

特に価格が安いものの、プッシュ型通信が必要となります。しかし、エンド・ツー・エンドの通信路さえあれば、管理しやすい形態です。

機器監視経路を構築する技術

IPv4 の現在の世界はプル型が中心です。しかし、監視経路を作る技術を徐々に適用していくことで、IPv6 によるプッシュ型のサービスに移行することができます。当初はポート転送を設定しますが、その後は特定アドレス、ポートの通信を手作業で許可する段階に移行し、最終的にはパケットフィルタリングの自動的な制御でプッシュを実現することができるようになるはずです。



IPv4 を利用した従来技術

IPv4 を利用するこれまでのやり方は、以下のような特徴を持っています。

プル型

イニシエータは常に LAN 内部のみで外部機器はなりません。実現が容易です。

プッシュ型

非 IP 回線、専用線、IP-VPN 網を利用する。端末を監視するだけのために異ネットワークを接続しています。したがって高コストであり、大規模な監視システムによる環境でなければ利用できません(SOHO では用いられにくい)。

ポートマッピングによるプッシュもあります。これは該当する内部ノードに対してポートフォワードを行うというものです。スケーラビリティを考慮する必要があります。また、ネットの管理にはある程度以上のスキルが必要です。

IPv6 化による従来技術の変化（BCP）

プル型

IPv4 利用の場合と変化はありません。

プッシュ型

非 IP 回線や専用線、IP-VPN 網などを経由してプッシュを行います。IPv4 利用の場合と変化はありません。インターネット上でも特別な設定なしに利用が可能（IPv6 の P2P 通信性）です。パケットフィルタ設定等のセキュリティに関する配慮は必要です。外部からの到達性を限定的に持たせるなどが考えられます。

しかし、スケーラビリティは低く、管理にはある程度以上の技術が必要です。エンド・ツー・エンドの IPSec トランスポートモード通信も適用可能です。

将来望まれる技術

将来望まれるのは、自由度の高いプッシュを実現する技術です。BCP において手作業で行っていた限定的な到達性実現を自動化し、相手の認証、フィルタへの穴あけ、利用完了後に穴を戻すような処理を自動的に実現するようなものです。これにより、相手（認証結果）や通信状況に応じた制御も可能になります。技術的には SIP に似たプロトコルになると思われます。

しかし、このようなプロトコルの手順は標準化する必要があります。 そうでないと、各メーカ独自規格が乱立し、メーカ、ユーザ共にコスト増となります。また、これによって他の方式の必要性が低下します。

トラブル要因と対策

v6fix、名前解決

v6fix

WIDE プロジェクトで、v6fix というプロジェクト（http://v6fix.net/）が発足しました。
これは、IPv6 に関する諸問題を解決するプロジェクトで、名前解決問題はこの活動においても重要なトピックとして扱われています。
ドキュメント化の取り組みとしては、InternetDraft が執筆されました。
draft-ietf-dnsop-misbehavior-against-aaaa-02
これはまもなく RFC になる予定です。
実施ガイドラインも http://v6fix/net/で公開準備中です。実態調査をまず日本国内で着手し、その後拡充されることになっています。実態調査の結果として、ベンダ、ドメイン管理者への改善依頼を予定しています。
また、実装クライアント側での対応用に、BSD のライブラリの提供が予定されています。

名前解決関係の現状

IPv6 実装状況

IPv6 は、多くの DNS サーバ、クライアントで実装済みです。
サーバでは、OS として BSD、Linux、Mac OS X など DNS は bind9, bind8.4 以降が IPv6 に対応しています。
クライアントでは、OS が WindowsXP、MacOS X、BSD、Linux など、ブラウザは Internet Explorer、Safari、Mozilla、Firefox が IPv6 をサポートしています。
こうしたことから、IPv6 接続性の有無に関わらず、AAAA の問い合わせが日常的に発生するようになってきています。

DNS の運用状況

DNS の IPv6 実装状況ですが、ccTLD サーバの半数以上（135/243 カ国）が IPv6 に対応しています。JP ドメインも数年前から対応済みです。gTLD(.com、.net)も、2004 年 10 月に対応しま

した。root サーバでの対応も進行中です。

AAAA に正しく反応しない DNS サーバ問題

この問題は、A RR しか持っていないドメイン（IPv6 を使っていない典型的なドメイン）に対して、AAAA RR に対する問い合わせを実施した場合の DNS の応答に関するものです。

正しい応答（RFC1034)

空の応答（エラーなし）を返す、あるいは AAAA RR は持っていないが、他の RR は持っていると返すのが正しい応答です。これにより、クライアントは別途、A RR の問い合わせを実施し、IPv4 で通信することができます。

間違った応答

AAAA の問い合わせを無視する DNS サーバが存在します。これにより、長いタイムアウトを生じます（数十秒から 1 分強）。

また、NXDOMAIN エラーを返すものもあります。これは、RR がないことを意味するため、IPv4 での通信もできなくなります。さらにレゾルバの DNS キャッシュに NXDOMAIN が残るため、AAAA を引かないクライアントも巻き添えになります。これがサービス妨害攻撃になる場合もあります（CERT 勧告）。

その他

ISP ユーザのトンネル利用への対応

ユーザのトンネル利用に対して ISP がどう対処するかという問題があります。具体的には IPv4 Protocol No.41 パケット(IPv6 カプセル化パケット)の扱いをどうするかという点です。

まず、トンネルサービスを行う場合には、ISP ネットワーク内ではこのパケットをフィルタリングしません。トンネルサービスを行わない場合でも、6to4 などの利用を妨げるので、可能な限りフィルタリングを行わないことを推奨します。

ただし、この場合、以下のインターネットドラフトに示されているように、セキュリティ的に弱い部分があります。

Security Considerations for 6to4
（http://www.ietf.org/internet-drafts/draft-ietf-v6ops-6to4-security-04.txt）

トンネル端点のあて先のみ IPv6 カプセル化パケットを通すなど、トンネルルータでのフィルタリ

ングが課題となります。

MTU ディスカバリについて

IPv4 パケットは、パケット配送の途中経路でも Fragment が可能で、ICMPv6 Type2 のような ICMP の利用はありません。このため、ISP など、ICMP パケットをフィルタリングするケースもあります。

しかし、IPv6 ではパケット配送における経路途中では Fragment が実施されません。経路途中のあるルータでパケットサイズが Too Big となった場合、そのルータが ICMPv6 の Type2 「Packet Too Big Message」を送信元に返します。送信元はそのメッセージを受け取り再度適切なサイズにパケットを収めて送信します。

このため、IPv6 インターネット上では ICMPv6 メッセージ（少なくとも Type2)がエンドノードまで配送されないと、通信性がそこなわれる場合があるので注意が必要です。
ISP を含めて、ICMPv6 Type2 メッセージはフィルタリングしない運用を徹底する必要があります（セキュリティガイドライン参照）。

インターネット関連技術情報

sTLA 割り振りの歴史的経緯

sTLA の割り振りに関する当初のポリシー(1999)では、初期割り振りの最小サイズが/35 となっていました。しかし、改定後(2002/7/1)は、初期割り振りの最小サイズが/32 となりました。これに伴い、すでに/35 を取得した sTLA 保持者は/32 へのアップグレードできることになりましたが、/32 への移行は任意であるため、新ポリシー後も/35 を保持する sTLA が存在しています。 したがって現在は、/32 、/35 の sTLA が共存しています（注：現在 sTLA という用語は使われていませんが、ここでは便宜上、RIR から直接アドレスの割り振りを受ける組織の意味で利用しています）。

IPv6 マルチキャストについて

マルチキャストとは、ルータがパケット中継時にパケットを 2 つ以上に複製することにより、1 台の送信者から N 台の受信者に対して効率的に情報を転送することを可能とする技術です。
ブロードバンドコンテンツのライブ中継や一斉配信などでの適用が効果的です。

マルチキャストを導入するにあたっては、適用する「経路制御方式」と「グループ管理方式」を選択する必要があります。

経路制御方式

マルチキャスト通信を実現するための、ルータ同士で利用されるプロトコルです。

PIM-SM

現時点で最も一般的な、マルチキャスト経路情報交換のためのプロトコル

PIM-SSM

受信者が送信者を指定した上でマルチキャストグループに参加できるようにするもので、不正な送信端末からのマルチキャスト通信阻害を防止可能

グループ管理方式

マルチキャスト通信を実現する為の、ルータとホスト間で利用されるプロトコルです。

MLD(Multicast Listener Discovery)

-MLDv1： PIM-SM 対応のマルチキャストグループ管理プロトコル

-MLDv2： PIM-SSM 対応のマルチキャストグループ管理プロトコル

現時点で適当なマルチキャスト方式とは

当面の実用化･普及面では、PIM-SM／MLDv1 が適切と考えられます。しかし、パケット転送効率、セキュリティ面では、 PIM-SSM／MLDv2 が優れています。

したがって当面は、PIM-SM と MLDv1 にて IPv6 マルチキャストを実現し、将来的に対応製品の充実に伴い、PIM-SSM と MLDv2 に移行するのが現実的です。

PIM-SM における BSR、RP

RP： 送受信ホストがマルチキャストへ参加するために参加メッセージを送信するルータのあるポイント。PIM-SM では、 通常時は RP を経由してマルチキャストパケットが転送される。

BSR： すべての PIM-SM ルータに対して、RP や BSR 自身の情報(IPv6 アドレスなど)を通知するルータ。

マルチキャストアドレス

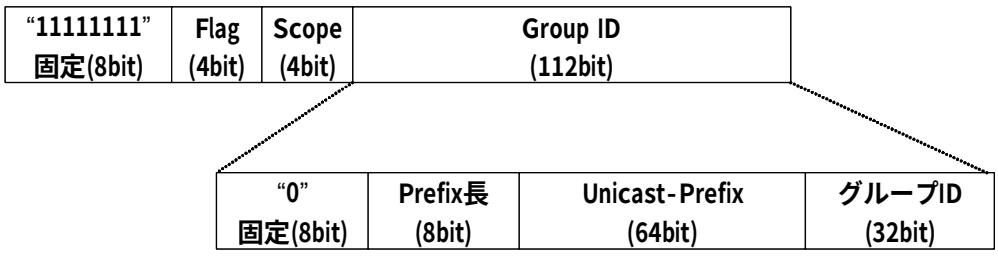
IPv6 では、マルチキャスト用のアドレス空間として、ff00::/8 が用意されています。参考として、IPv4 の場合は、224.0.0.0～239.255.255.255(クラス D)がマルチキャスト用アドレスです。

このアドレス空間の利用方法は、たとえば 2001:db8:1234::/48 を有するユーザが、マルチキャストアドレスを生成する場合、次のようになります。

ff3x:30:2001:db8:1234::****:****

x： スコープ指定

*： グループ ID 指定



特殊な IPv6 マルチキャストアドレスとしては、以下があります。

ff02::/16 ： リンクローカルスコープのマルチキャストアドレス

ff0e::/16 ： **グローバルスコープのマルチキャストアドレス**

IP 網の通信品質保証

IP 網における通信品質保証手段としては、以下が考えられます。

・物理的な手段（帯域増加、収容数制限）
・ATM、SONET、Ethernet 等においてネットワーク機器の機能で実現する（キューイングのスケジューリング、TDM（ATM, SONET)、優先度パケット廃棄）
・機器の動的設定には、VLAN 機能、シグナリング(RSVP 等)や管理サーバからの設定(COPS 等)を用いる

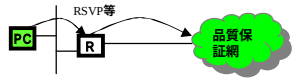
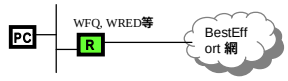
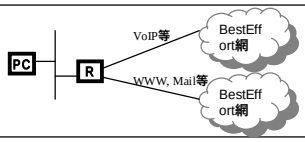
通信品質保証は、QoS と CoS に大別されます。品質の基準（パケット廃棄、遅延、帯域、ジッタ等）は多種多様です。

QoS：Quality of Service
通信に対して資源（帯域等）を確保し、通信品質を保証する。リアルタイムアプリケーション等が対象
CoS：Class of Service
通信品質を優先度を用いて保証する。業務アプリケーション等が対象

SOHO の通信品質保証パターン

SOHO では、下表のような通信品質保証が考えられます。これらは必ずしも単独で利用する必要はなく、組み合わせて活用することもできます。

SOHOの通信品質保証パターン

項目	内容	概要図
端末	端末主導の通信品質保証システムを利用する。	
接続回線	Routerにて品質保証設定（優先転送やパケット廃棄）を行う。接続回線帯域増加も含む。	
複数接続回線	複数の接続回線を利用し、負荷を分散させる。	
通信品質保証網	キャリアが通信品質を保証した網を用意する。	

上記パターンを単独あるいは組み合わせて利用する。

IPv6普及･高度化推進協議会　移行WG

SOHO の通信品質保証

LAN

LAN においては、Gigabit Ethernet 機器等の低価格化により潤沢な帯域を利用可能であるため、品質保証技術の要望は少ないと言えます。

WAN

WAN 接続の回線速度は、数 Mbps～100Mbps 程度であり、LAN 内と比較して遅く、品質劣化の原因になりやすくなっています。これについては、マルチホームによるインバウンド/アウトバウンドのトラヒック分散手法を取り入れることも可能です。

キャリアの内部網では、基本的にベストエフォートであるため品質は保証されません。しかし、保証する際には、CE（カスタマエッジ）においてアウトバウンドのトラヒックの制御を行う手法や通信品質保証可能な機器で網を構築し、機能提供する手法があります。

IPv6 の品質保証に関する特徴

IPv6 のヘッダフォーマット

IPv6 ヘッダには、品質保証に関して 2 つのフィールドが設けられています。

Traffic Class フィールド（8bit）
優先制御等のクラス分類に使用する。IPv4 では、ToS(Type of Service)（8bit）である
Flow Label フィールド（20bit）
送信元がフロー単位の処理方法を指定するのに使用する

ネットワーク側でのパケット分割回避

IPv6 では、通信経路上の機器によるパケット分割は行われません。しかし、これに関しては留意点があります。

送信端末が、廃棄されないサイズのパケットを送信するためには、より小さい MTU が設定された経路上の機器から送信元へ、ICMP の「Too-Big-Message」が到達する必要があります。

この場合、経路の機器を管理する ISP 等が該当メッセージを遮断しないことや遮断しないことによるセキュリティ低下について検討する必要があります。

IPv6 の事象別特徴

IPv6 は、IPv4 と比較した場合、下表のような品質保証上の特徴があります。総じてより細かく、自由度の高い制御が可能です。

IPv6の事象別特徴

項目	IPv4	IPv6
アプリケーションの通信品質保証	IPレイヤにて8bit（ToS）種類が制御可能	IPレイヤにて8+24bit（Traffic ClassとFlow Label）種類が制御可能
端末単位の通信品質保証（VoIP, リモートメンテナンス等）	NAT利用のアドレス隠蔽により、E2EのQoS保証は困難	グローバルアドレス利用によりE2EのQoS保証が容易
端末自身による資源誘導	予め、資源へ経路設定を行う静的な資源誘導あるいはRSVP等のシグナリングを利用。	マルチプレフィックスによるソースアドレスセレクションを用いた動的な資源誘導
パケット分割による処理遅延回避	通信経路上でパケット分割や再構築が行われるため、処理遅延増加	送信元以外ではパケット分割をしないため、経路上での処理遅延低減

- IPv6は、QoS保証の粒度がより細分化でき、自由度の高い設定（E2EのQoSのマッピング等）が可能である

通信品質保証まとめ

IP の通信品質保証は、構成される物理網に大きく依存します。そして、IPv4 から IPv6 へ移行する際に物理網が変化することはないため、品質保証技術そのものに差異はないと考えられます。

しかし、IPv6 は、IPv4 と比較すると、品質保証に関して粒度細分化や E2EQoS、資源誘導、パケット分割に関して優位性があります。IPv6 を用いることで、特に VoIP やリモートメンテナンスといった E2E を対象とした品質保証実現が容易になります。このため、E2E 上の全構成要素を連携した品質保証も可能となります。

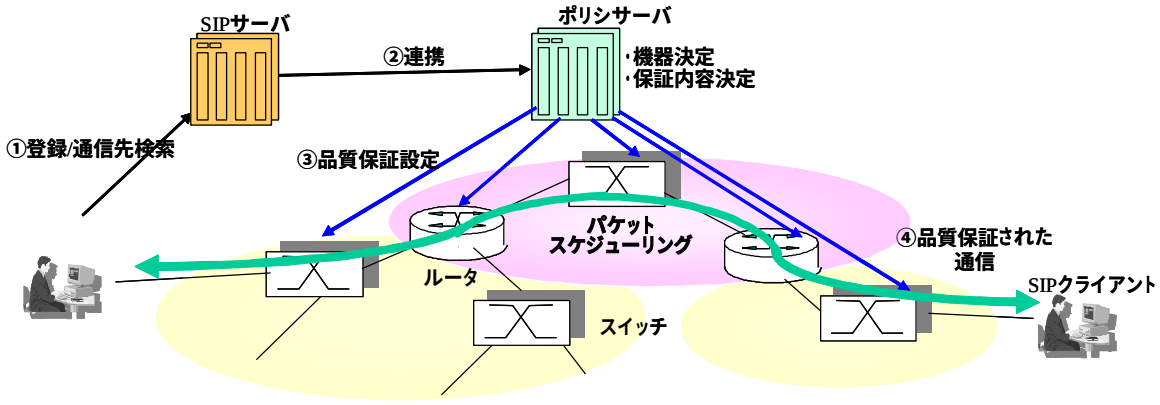
ただし、SOHO では、品質保証の設計・設定・運用を行う管理者がいないことが課題です。

通信品質ガイドライン

IPv6 移行にともない、全通信を IP 網に頼る SOHO においてミッションクリティカルな通信とその他通信を差別化し品質保証を行うことは必須となります。

IPv6 により品質保証の細分化が向上します。しかし、管理者不在の SOHO では、LAN での品質保証は比較的容易ながら、WAN の品質保証は困難です。

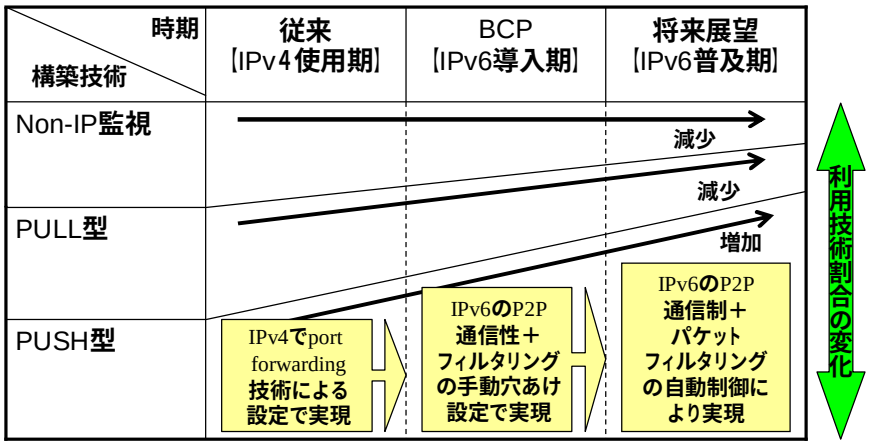
そのため、SOHO に対して、自動化された通信品質保証が提供される必要があります（注：品質保証サービスが従量課金か定量課金かのどちらになるかは、利用方法により異なります）。



機器監視経路を構築する技術の推移

機器の監視経路を構築する技術については、遠隔監視・遠隔制御の項でも説明されていますが、下表のように、徐々にプッシュ型の機器監視が増えていくと考えられます。

機器監視経路を構築する技術の推移



IPv6普及・高度化推進協議会　移行WG

インターネットシステムの IPv6 対応状況

サーバの分類

ISP におけるサーバは、以下のように分類できます。

サービスサーバ

利用者が実際に使用するアプリケーションサーバで、Web、メールなどがあります。用途に応じて種々のカスタマイズが施されており、たとえば、ISP 広報用 Web、ホスティング、接続サービスにバンドルされる Web やメールなどがあります。

インフラサーバ

サービス利用にあたり共通的に必要となるサーバで、DNS や Radius がこれにあたります。最も信頼性が要求される部分です。

運用サーバ

ISP 運用に必要となるサーバで、NMS、SNMP などです。利用者が直接アクセスする対象ではなく、IPv6 対応は必須ではありません。

サーバの IPv6 対応

現在のサーバの IPv6 対応の状況としては、まずサーバとして使用されている OS の多くはデュアルスタック構成可能（Linux, FreeBSD, Solaris 等）です。アプリケーションについては、既存の IPv4 アプリケーションの殆ど（Web、メール、DNS 等）が IPv6 対応を完了しています。DNS、Web に関しては、ISP の商用・実験サービスでの提供実績がすでにあります。

IPv6 対応手法

サーバの構成方法としては、IPv4 サービスサーバのデュアル化、IPv6 サービス専用サーバの新規追加の 2 通りが考えられます。デュアル化により IPv4 パフォーマンスに影響が払拭できないケースでは後者を選択します。デュアル化の際、OS、アプリのバージョンアップによりサービス断の影響が大きい場合も同様です。

サーバは、IPv6 サービス専用の新規デュアルセグメントに設置します。これは、脆弱性等の対応速度が異なるであろう IPv6 サーバと IPv4 サーバを同一セグメントに収容した場合、IPv4 サーバに影響が及ぶ可能性があるからです。これは、バックボーンに比べるとそれほど大きなコスト要因ではありません。

IPv6 サーバセグメントでの ICMPv6 のフィルタリングには注意が必要です。IPv6 でのフラグメント処理は、中間ノードでは行わず、Path MTU Discovery（ICMPv6 type2 メッセージを使用）により、送信元端末が配送可能なサイズに分割するため、途中のルータで ICMPv6 type2 メッセージをフィルタしてはなりません。

DNS

DNS の IPv6 対応には、IPv6 アドレスが解決できることと、それが IPv6 経由で実行できることの 2 つの側面があります。IPv6 での名前解決には、ホスト名から IPv6 アドレス（正引き、AAAA レコード）、IPv6 アドレスからホスト名（逆引き、ip6.arpa.ドメイン）の 2 つがあります。

利用する DNS 実装については、BIND9 を推奨します。BIND9 では、IPv6 を完全にサポートしています。商用提供により、実績も積まれています。ただし、BIND8 でも同じことは可能になりました。また、名前解決のみなら BIND4 でも OK（IPv4 経由）です。

ISP における IPv6 対応の方法としては、もっとも重要なサーバでサービス断は許されないため、IPv6 用に新規にデュアルサーバを 2 台用意します（プライマリ、セカンダリ）。リゾルバとゾーン管

理は兼用でもかまいません。

これを IPv6 専用リゾルバとして提供します。IPv4 経由の問い合わせは既存のサーバを利用してもらいます。また、顧客の要望に応じて、逆引き委譲や、顧客の管理する DNS のセカンダリとしての提供も行ないます。

Web

Web サーバは、ISP の広報用 Web、接続サービスにバンドルされる Web、Web ホスティングに分類されます。ソフトウェアの対応については、Apache2.0 以降で標準対応済みで、ISP での利用実績もあります。

対応方法としては、まず ISP の広報用 Web から対応すべきです。DNS に比べるとクリティカルなものではないですが、安全性を重んじる場合にはデュアルスタックのサーバを新設します。Apache2.0 以降であれば既存のサーバをデュアル化する手もあります。

ISP サービスにバンドルされる Web と Web ホスティングのデュアル化はもう少し先になりそうです。これは、中小 ISP の場合、ホスティング事業者のサービスを利用しているケースが多く、そのホスティング事業者のデュアル化がまだだという事情によるからです。

自力による解決策として、新規にデュアルサーバを新設した場合が考えられますが、サーバの数が多く、コンテンツの移設に稼動がかかるほか、コンテンツのミラー、同期の仕組みも必要となり運用工数が増す問題が生じます。

一方、現実的な解として、デュアルスタック化したリバースプロキシの設置があります。これにより、IPv6 から IPv4 の既存サーバへのアクセスを提供することが可能となる他、コンテンツの移設も考慮しなくてよいため、IPv6 アクセスの少ない段階ではよい解決策になります。

Mail

メールサーバのソフトウェアについては、Sendmail8.1 以降で IPv6 に標準対応しています。Qpopper は IPv6 対応パッチで対応可能です。ただし、DNS、Web と比べ、利用実績は少ないと言えます。

現状の BCP としては、ウィルス駆除ソフトが IPv6 未対応であるため、ISP サービスとしての提供は控えるべきです。つまり、現状では、SMTP、POP サーバを IPv6 対応にしない、DNS の MX レコードのホスト名に IPv6 アドレスを持たせない、という対策を行います。

上記の問題がクリアされた場合の IPv6 対応方法としては 2 通りがあります。まず、既存のメールアカウントで行う場合、デュアルサーバを新設し、既存の IPv4 サーバのディスクを NFS 等で共有します。また、新たなメールアカウントを用いる場合、デュアルサーバを新設します。

監視（NMS、SNMP）

運用サーバ（NMS、SNMP）の IPv6 対応については、当面デュアルスタックネットワークが前提（ISP は特に）との考えから完全に IPv6 対応した製品は少ない状況です。特に SNMP の IPv6 トランスポートは、マネージャ、クライアントともに実装が少ない状況です。しかし、IPv6 MIB が IPv4 経由で取得できればそれほど深刻とはなりません。

到達性チェックについては、接続性（ping）監視は IPv6 で行う必要があり、商用ツールも対応済みです。

サービスチェックは IPv6 で行う必要がありますが、商用ツールは現状では未対応です。フリーで使えるものがあります（Nagios）。

現状の多くの ISP は、IPv6 サービス用に新規デュアルサーバを設置しています。

お問い合わせ先

本ガイドラインに関するお問い合わせは、以下のアドレスまでメールでご連絡下さい。

IPv6 普及･高度化推進協議会移行 WG／e-mail: wg-dp-comment@v6pc.jp