# IPv6 移行ガイドライン
## (家庭セグメント)

2004 年 5 月

IPv6 普及･高度化推進協議会

移行 WG　家庭 SWG

# 目　次

# はじめに

本ドキュメントは、家庭向けの IPv6 機器の開発に携わるベンダーやサービス提供者を対象に、家庭内のネットワークに IPv6 機器を導入する際に、検討すべき一般的な項目、指針、方法について記述しています。

ここで記載される内容は、考え方の例を示すものであり、唯一の解ではありません。読者が、自らの指針により IPv6 の導入を検討する際、このドキュメントを参考に応用が図れること意識して記述しています。

## ■SWG 参加メンバー

### チェア

久保田（松下電器）

### 検討メンバー

荒野（インテックネットコア）
石原（東芝）
小澤（松下電器）
尾上（松下電器）
川島（NEC アクセステクニカ）
菊山（松下電器）
貞田（NTT コミュニケーションズ）
島田（松下電器）
鈴木（松下電器）
瀬川（パナソニックコミュニケーションズ）
中井（NTT コミュニケーションズ）
中村（松下電器）
村田（パナソニックコミュニケーションズ）
山谷（アライズ）
（敬称略、あいうえお順）

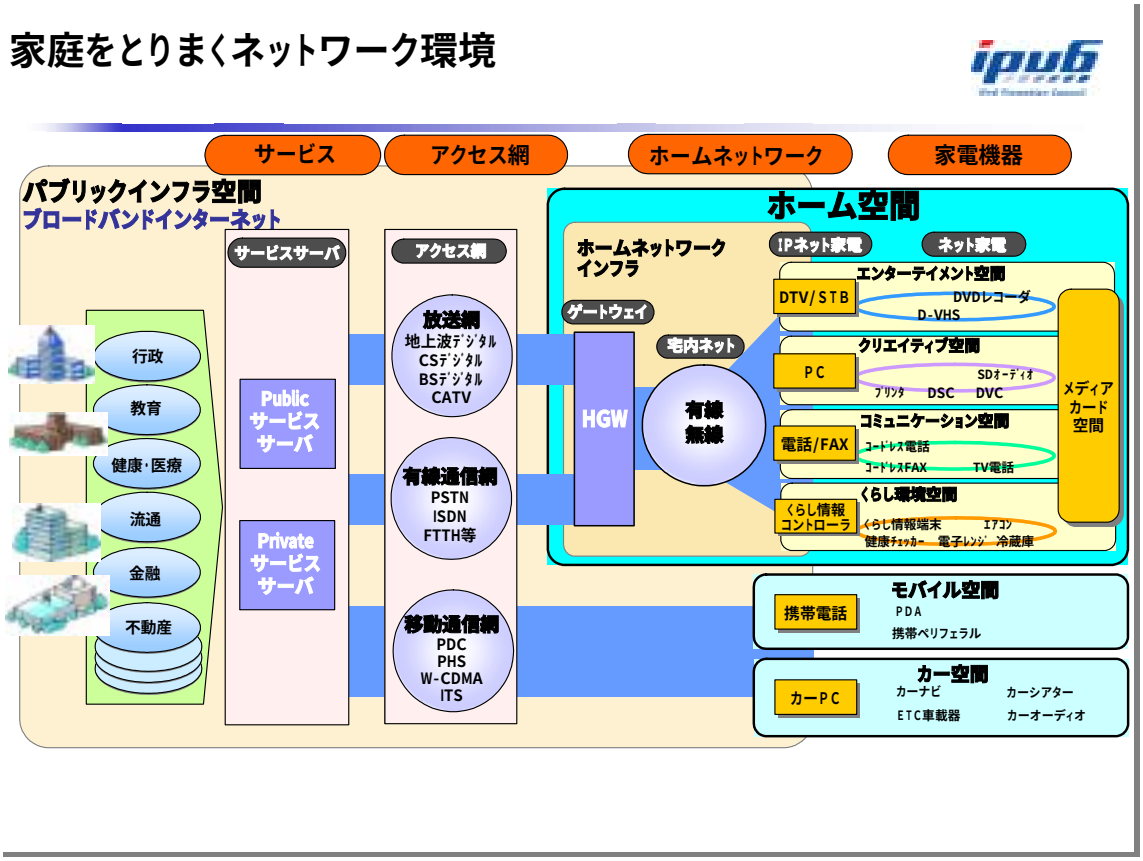
## ■お問い合わせ先

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を下さい。

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

# 1. セグメントの特徴

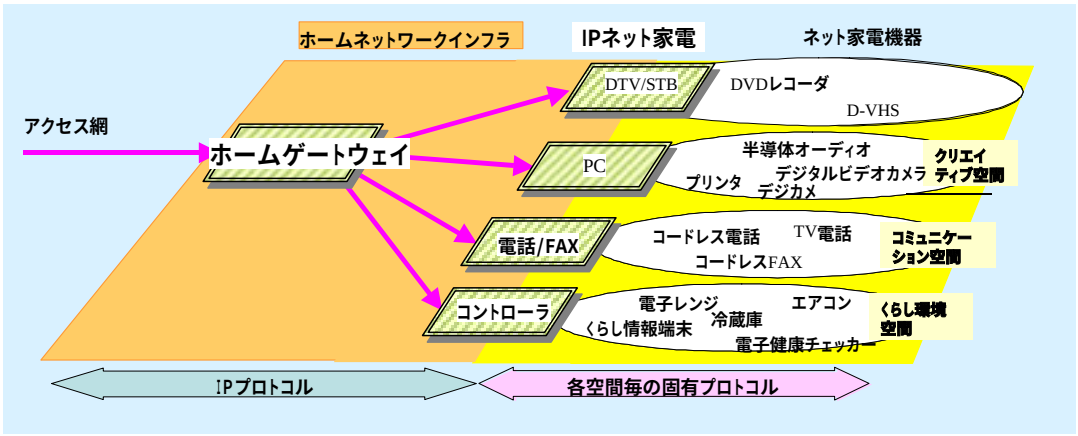
## ■家庭をとりまくネットワーク環境




日本のブロードバンド世帯普及率は 30 パーセントにも達し、家庭は確実にいつでもインターネットとつながる状況になってきています。接続方法も ADSL、CATV インターネット、FTTH など多様化しています。今後はネット家電の本格化、テレビ放送のデジタル化、インターネット電話の進展などにしたがい、さらにネットワークが人々の生活に溶け込んでいくことが考えられます。これまでは、情報収集などの目的を持ち、意識的にインターネットにつなぎにいくのが中心でしたが、これからは外から家庭の機器が操作できるとか、取りためた静止画や動画を他の家庭に見せるとか、データ通信ということをあまり考えない利用形態も進んでいくでしょう。インターネット上の一般家庭向けサービスも、これまでのパソコン向けとは違ったものが次々に登場するに違いありません。

## ■家庭セグメントの特徴

### ホームネットワークのアーキテクチャの例




- ホームゲートウェイ（家庭用ルータ）がアクセス網と接続
- 各機器群内で各種プロトコル（IEEE1394・USB・Echonetなど）を利用
- 各機器群のなかに、IPと個別プロトコルの変換をする機器（IPネット家電）が存在する場合がある
- 将来的には、nonIPな機器のIP化が進んでいくことが考えられる

現在から将来にかけての家庭セグメントの特徴としては、次のような点が考えられます。

・1 軒ごとにネットワーク構成や利用機器が異なる
・特に今後は、PC だけでなく Non PC 機器（白物家電・AV 機器）が存在するようになる
・ネットワークを管理できる人がいない
・家庭ユーザに細かい設定は期待できない
・デフォルト、あるいは一度設定したままで使い続ける
・機器、特に家電は設定用のインタフェースを持たないこともある
・ISP の接続サービスを利用
・ホームネットワークは当面 1 セグメントを前提
・基本的なネットワークニーズは、SOHO と大きくかけ離れることはない

なお、以下では、IP を終端する機器を対象とし、非 IP な機器・ネットワーク（Echonet や IEEE1394 など）は範囲外とします。

# ■現状の分析

## (1) 現状の家庭におけるインターネット接続・利用状況

インターネットとの接続方法別加入者数は、以下の通りです（統計データは 2003 年 12 月：総務省）

・ダイアルアップ加入者数　約 1918 万
・PC（モデム）より直接ダイアルアップ（PSTN）あるいはダイアルアップルルータ（ISDN）
・常時接続環境加入者数　約 1364 万[ADSL（1027 万）/FTTH（90 万）/CATV（247 万）]
・携帯電話によるインターネットサービス加入者数　約 6780 万
（日本の総世帯数：約 4600 万：2000 年）

インターネットに接続している機器は、ルータ（ホームゲートウェイ）、PC がほとんどですが、AV 機器についても単体・個別サービスが一部で開始しています。また、白物家電を対象としたネットワークサービスも一部メーカより試験的に登場しています。ただし、普及はまだ当面先と考えられます。さらにネットカメラやセンサー系の機器が使われ始めていますが、数はまだまだ少ないのが現状です。

## (2) 家庭内ネットワーク配線

家庭内のネットワーク配線は、一般的にイーサネットケーブルか 802.11a/b/g といった無線 LAN を利用しています。

## (3) 利用サービス

そして、インターネットの利用用途としては、Web ブラウザによる Web 閲覧や、メールクライアントソフトを使って ISP などのメールサーバ経由でのメールのやり取りが一般的です。一部のハードディスクビデオレコーダでは、外出先から家庭に置かれた機器に対して遠隔的に録画予約を行なえるような機能が提供されています。

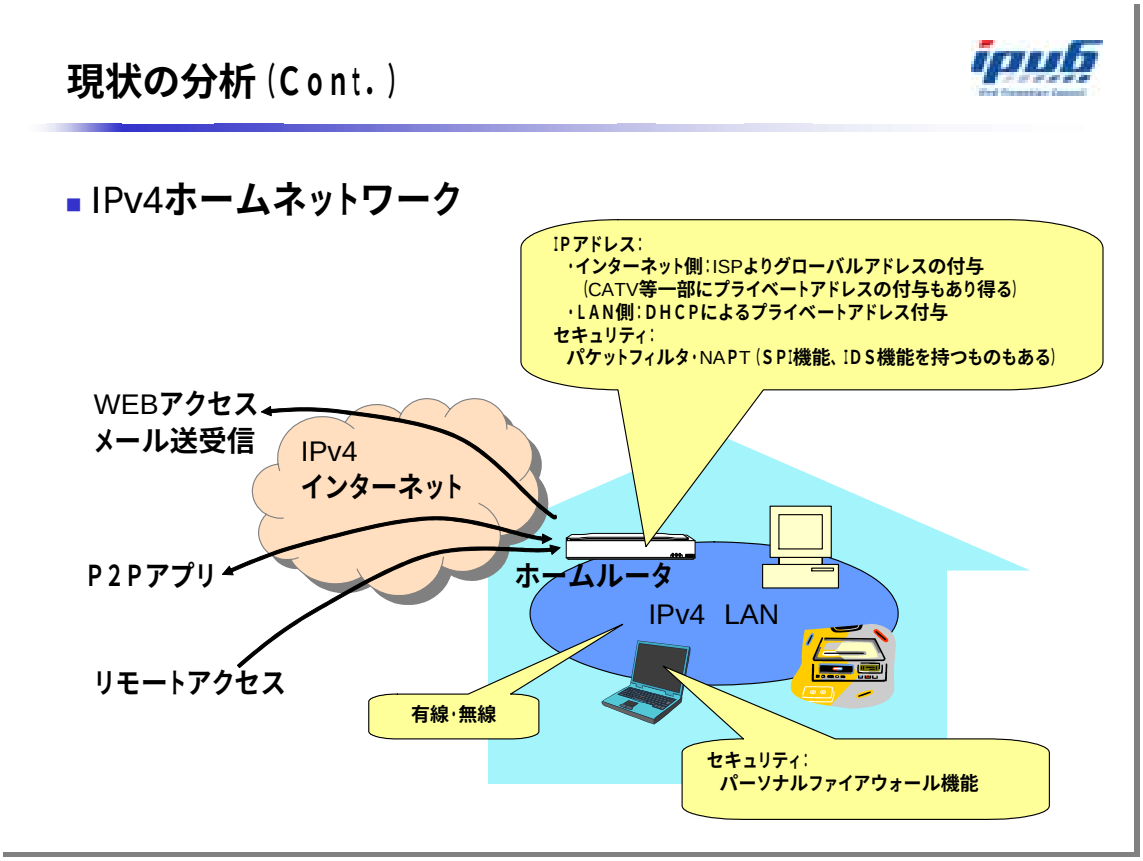
## (4) セキュリティ

現状における家庭ネットワークのセキュリティ確保は、おもにルータで行われています。家庭用ルータのセキュリティ機能は、パケットフィルタリングと NAPT 機能といった簡単なものが中心ですが、一部の製品ではステートフルパケットインスペクションや不正侵入検知機能が搭載されています。

PC にウイルスチェックソフトを入れているユーザはかなり増えており、パーソナルファイアウォール製品は一部のユーザで使われています。ISP によるメールのウイルスチェック・サービスも使われ始めています。

しかし、大多数のユーザはパケットフィルタリングと NAPT によるセキュリティに留まっており、ほとんどのユーザはすでに提供されている機能以外は利用しません。

## (5) IPv4 ホームネットワーク




主に利用されているネットワークプロトコルは IPv4 で、アドレスについては ISP よりグローバルアドレスを 1 つ受け取り、家庭用ルータに割り当てて、家庭内では DHCP によりプライベートアドレスを割り当て、プライベートアドレスとグローバルアドレスとの変換は家庭用ルータが実行するという形態が一般的です（CATV インターネットサービスの一部では、家庭用ルータに対してもプライベートアドレスが割り当てられています）。

セキュリティについては家庭用ルータのパケットフィルタリング機能（場合によってはファイアウォール機能）や PC 上のパーソナルファイアウォール機能が利用されています。利用アプリケーションは Web、電子メール、そして一部のユーザは活発にファイル交換ソフトを利用しています。

## ■家庭における IPv6 利用シーン

では、こうした一般の家庭が IPv6 を利用し始めるきっかけとなるものは何でしょうか。現状では一般に利用されうるキラーアプリケーションやキラーサービスといったものは存在していません。したがって、IPv6 移行への最初のきっかけを、以下では端末ベンダーにおける IPv6 端末開発ニーズ、そしてユーザ側の 5 つのインターネット利用シーンに分類して考えていきます。

### (1) 端末ベンダーにとっての IPv6 端末開発のニーズ

端末ベンダーにとって、IPv6 端末を開発するインセンティブは、以下のようなサービスを実現できることにあります。

**①放送サービス型**

サービスプロバイダが放送のようなサービスを提供し、それを受信するための端末が必要となります。たとえばビデオ放送や、遠隔メンテナンス、遠隔監視、検針などの閉じた形のサービスが考えられます。

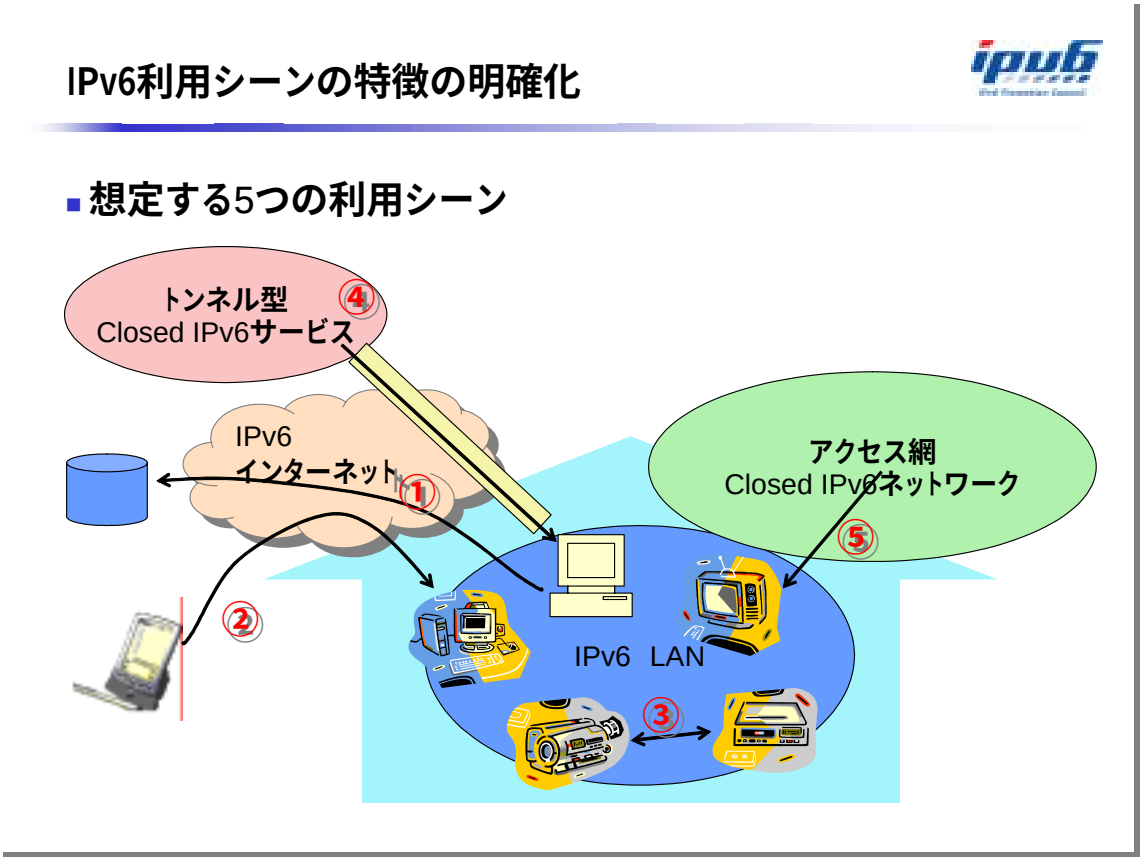
**②ヘビーユーザ型**

IP ユーザが IPv6 のメリットを活用していくにつれ、ユーザニーズの発展型として専用端末が必要となります。例としては、ホームサーバ、VTR、チャット、TV 会議などが考えられます。

**③家電間通信型**

家電同士が通信するためのプロトコルとして IPv6 を採用します。この場合、家に閉じない利用方法となります。機器ベンダーの選択により IPv6 を使った端末を開発することが考えられます。カメラとプリンタ、カメラと TV、TV チャット端末、冷蔵庫と TV などの間の通信を実現します。

## (2) ユーザ側の IPv6 利用シーン




ユーザ側の IPv6 利用シーンとして、以下では、図のような 5 つの利用シーンを考えていきます。

**①IPv4 同様の世界へのコネクティビティ**
Web やメール、WMP での映像視聴が中心
新しいところで白物家電からの Web アクセス、ファームウェアアップデート等

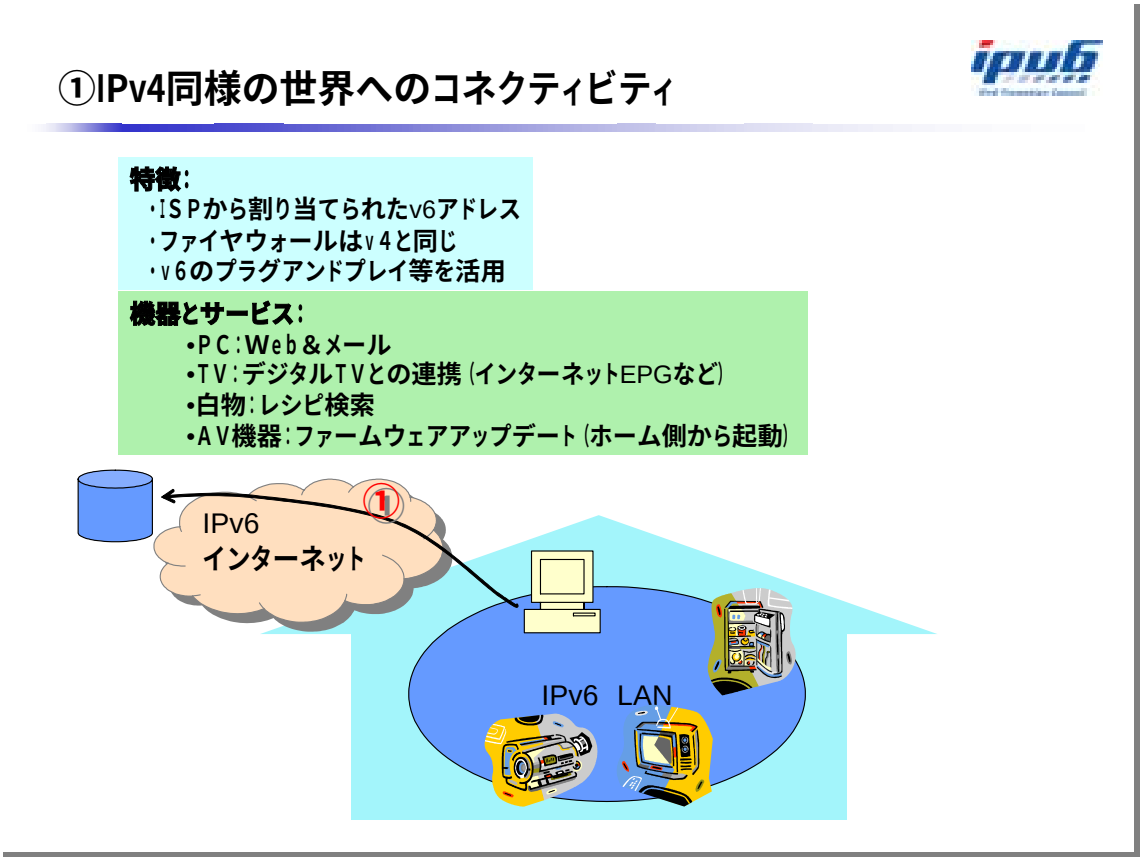
**②外から中へのアクセス**（個人の意思で IPv6 を利用）
ホームビデオサーバへのアクセス、Web カメラ、エアコン操作等

**③LAN 内での機器同士の通信**（家電メーカが IPv6 を選択）
TV とビデオの接続、インターネット＋VPN 越しで親戚間でビデオチャット等

**④トンネル上で遠隔サービス提供**（サービス事業者が IPv6 で提供）
機器の遠隔メンテナンス、TV への文字放送、専用機器で自治体サービス等

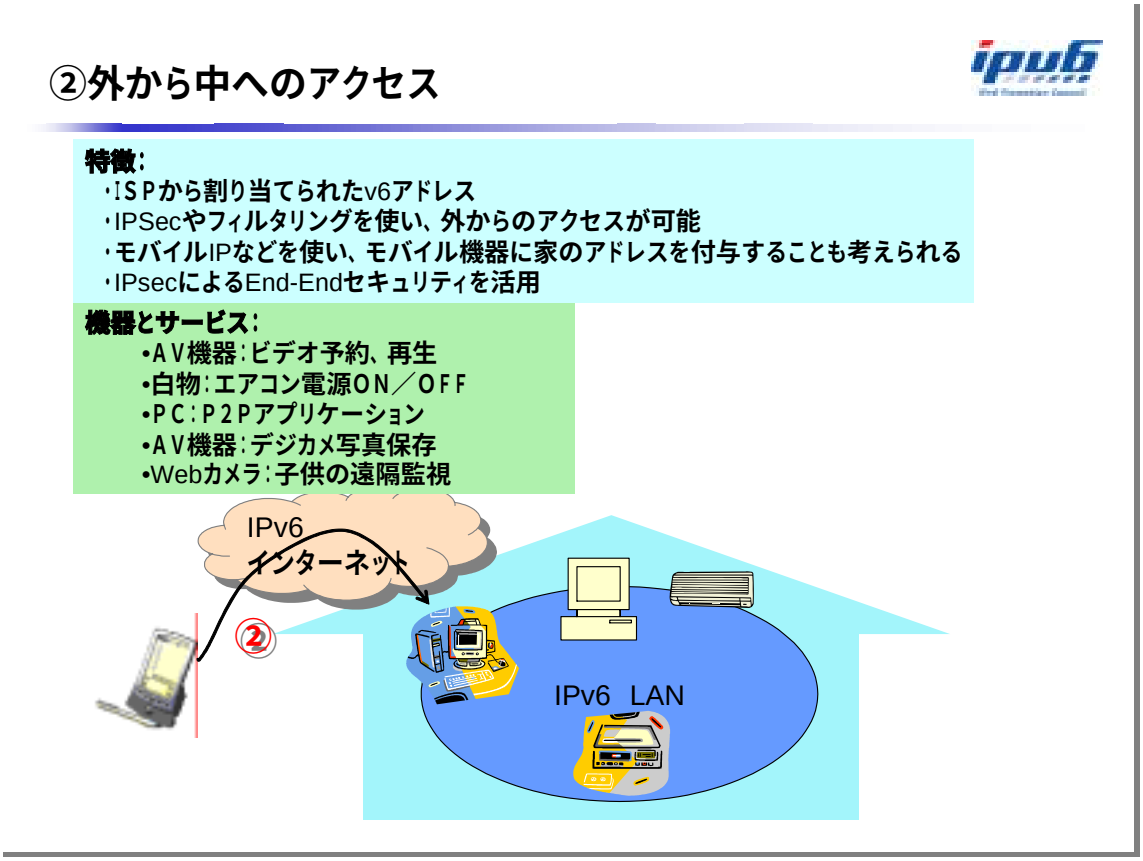
**⑤アクセス網に閉じたクローズドサービス**（回線事業者が IPv6 提供）
マルチキャストでの TV 映像配信、QoS 保障が必要なクリティカルな通信等

## ① IPv4 同様の世界へのコネクティビティ



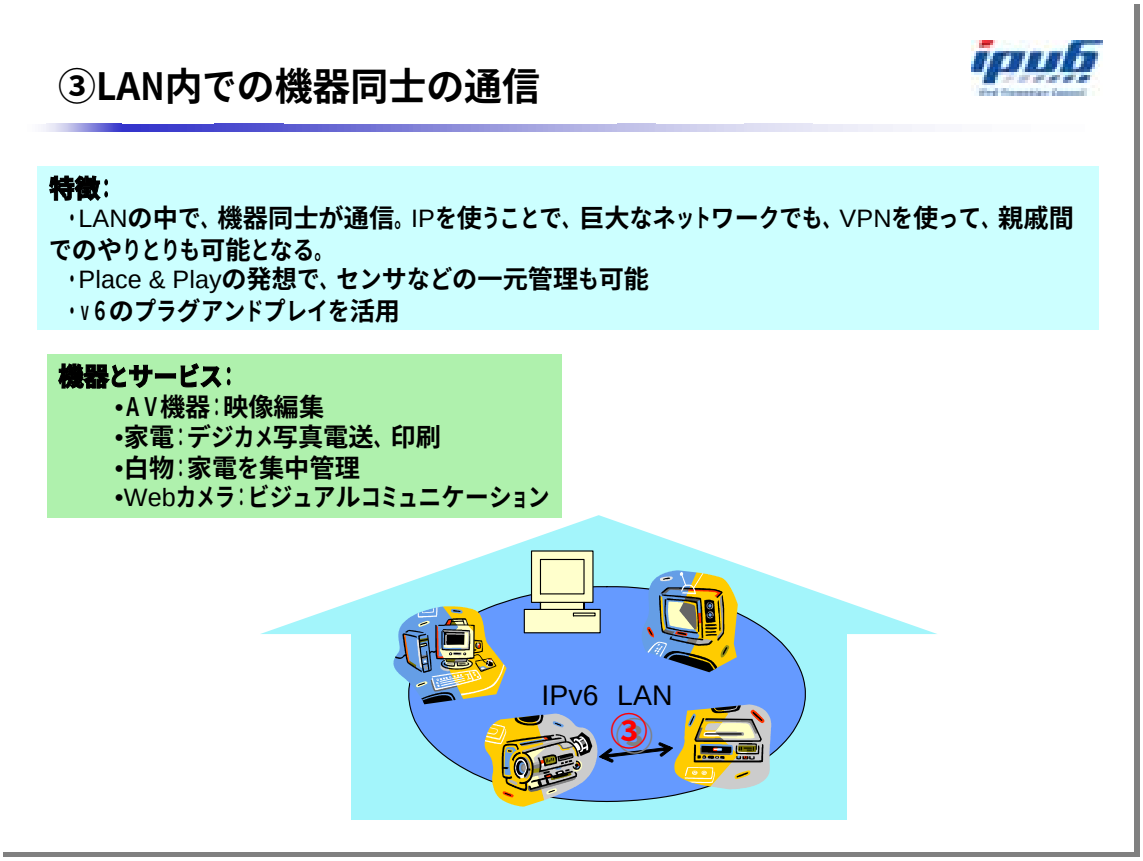

ここで想定されるのは、現在 IPv4 で利用されているのと同様のアプリケーションです。PC では Web と電子メール、テレビではインターネット EPG などのデジタル TV との連携、白物家電ではレシピ検索、AV 機器ではファームウェアアップデート（ホーム側から起動）が考えられます。IPv6 でこれらのサービスを提供する場合には、ISP から割り当てられた IPv6 アドレスを使い、一部で IPv6 のプラグ・アンド・プレイ機能を活用します。

## ②外から中へのアクセス



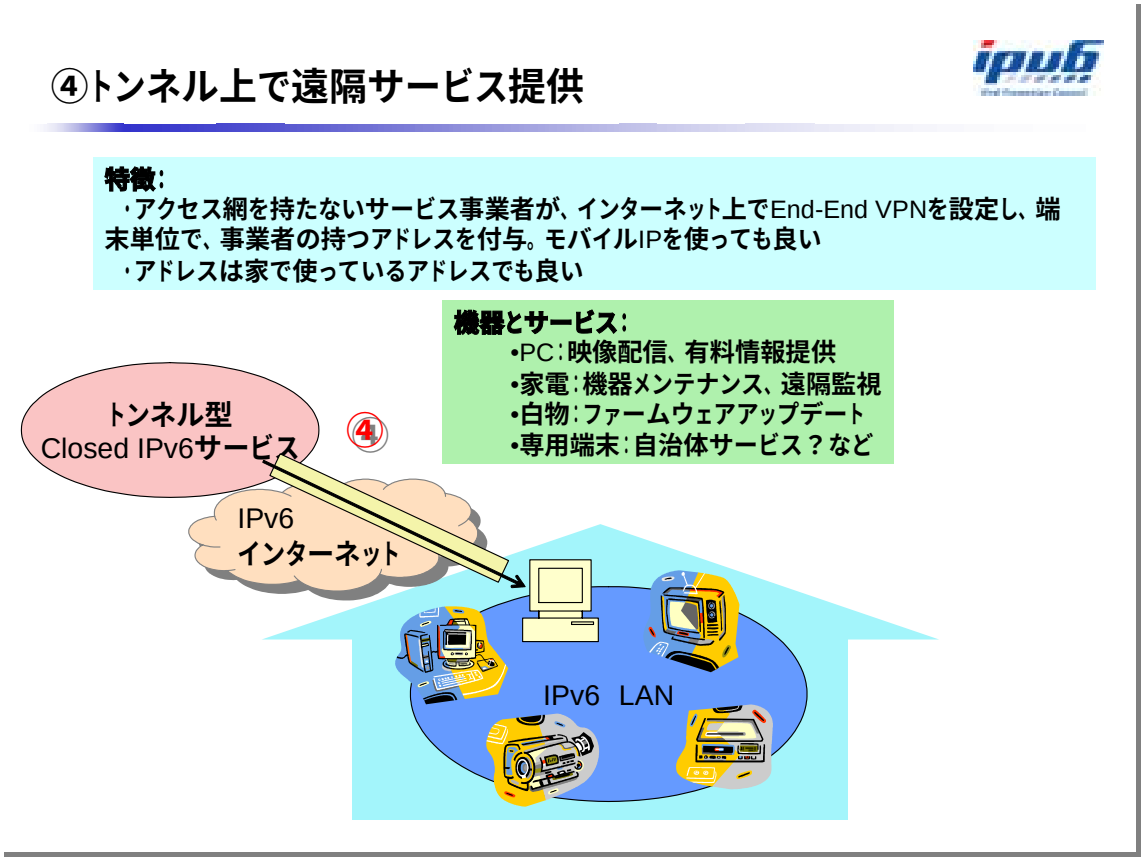

これはネット家電のメリットとしてよく語られるものの 1 つです。用途はビデオの予約・再生やデジタルカメラの写真の保存、エアコンの電源オン・オフ、パソコンでは P2P アプリケーション、Web カメラによる子供の遠隔監視などです。この場合、IPsec やフィルタリング設定によってセキュリティを確保することが考えられます。IPsec は、家庭内の機器とエンドツーエンドで使われる場合もありえます。一部では Mobile IP が利用されるかもしれません。

## ③LAN 内での機器同士の通信



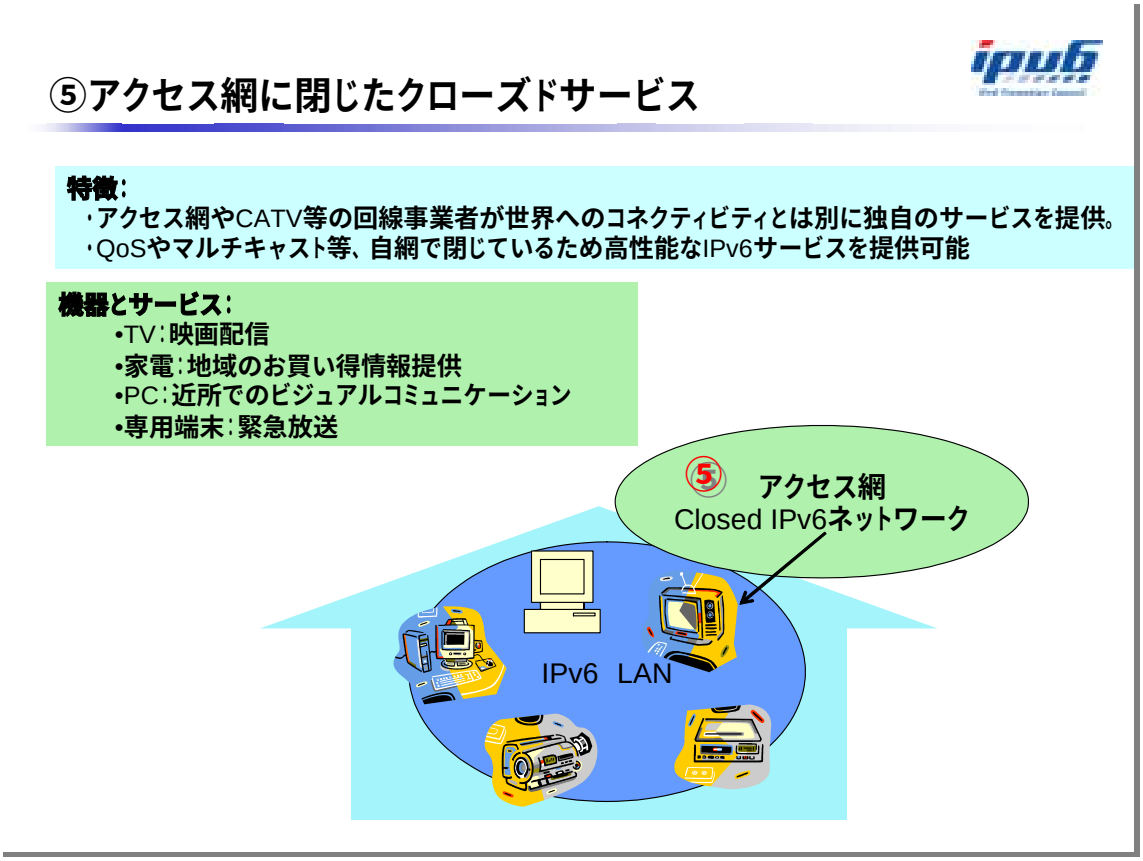

家庭内で家電同士がネットワークでつながることにより新たなアプリケーションが生まれます。映像編集やデジタルカメラの印刷、白物家電の集中管理などです。この場合、LAN とは家庭のことですが、VPN 接続で家庭間をつなぐことにより、親戚との間で Web ビデオカメラを使ったコミュニケーションなども可能になります。同じ接続形態で、センサーなどを一元管理することもできます。

## ④トンネル上で遠隔サービス提供




アクセス網を持たない事業者によるサービス提供で IPv6 が使われる可能性もあります。そのサービスとしては、PC に対する映像配信や有料情報の提供、家電のメンテナンスや遠隔監視、白物家電のファームウェアアップデート、専用端末による自治体サービスなどが考えられます。こうした場合のネットワーク構成としては、利用者の IPv6 アドレスをそのまま変更せず、インターネット上でエンドツーエンドの VPN を設定するか、Mobile IP を利用し、端末単位で事業者の持つアドレスを付与できます。

## ⑤アクセス網に閉じたクローズドサービス




アクセス網や CATV 等の回線事業者が世界へのコネクティビティとは別に独自のサービスを提供することが考えられます。この場合、QoS やマルチキャスト等、自網で閉じているため高性能な IPv6 サービスを提供可能です。用途としては、映画配信、テレビなどに対する近所のお買い得情報配信、専用端末を使った緊急放送などがあります。

## ■利用シーンに向けた移行のモデル・シナリオ

以下では、これら5つの利用シーンにおけるIPv6への移行の方法や課題を取り上げますが、大まかには次のようなことが指摘できます。

まず①については、IPv4でできることがIPv6でできるのは当然のことと言えます。また、⑤についても、当面のサービス形態として有力である可能性があります。③については、物理的に接続される場合とVPNにより仮想的に同一LAN内として接続される場合がありえますが、これも実現できることが望ましいと考えられます。技術的には、②における課題が解決できれば、すべての利用シーンにおける課題が解決できると考えられます。

では、家庭セグメントにおいてIPv4とIPv6が5対5の状況とは、どのようなものになるでしょうか。家庭内には、IPv4とIPv6の機器が混在します。利用アプリケーションとしては、Webや電子メールだけでなく、家庭内で機器連携をベースにしたサービスやアプリケーションが使われます。そして、家庭外・リモートから家庭内の機器を操作・監視できるサービスやアプリケーションも開始され、ユーザに対してできるだけIPv4やIPv6を意識させないでサービスを提供できることが求められます。つまり、5対5を目指して行なうべきことは、②の利用シーンにおける課題をクリアすることであり、以下ではこのシナリオを検討していきます。

# 2. 移行モデルとシナリオ

## ■移行モデルとシナリオの考え方

以下では、まず現在の家庭の状態として、以下の 3 種類を想定します。

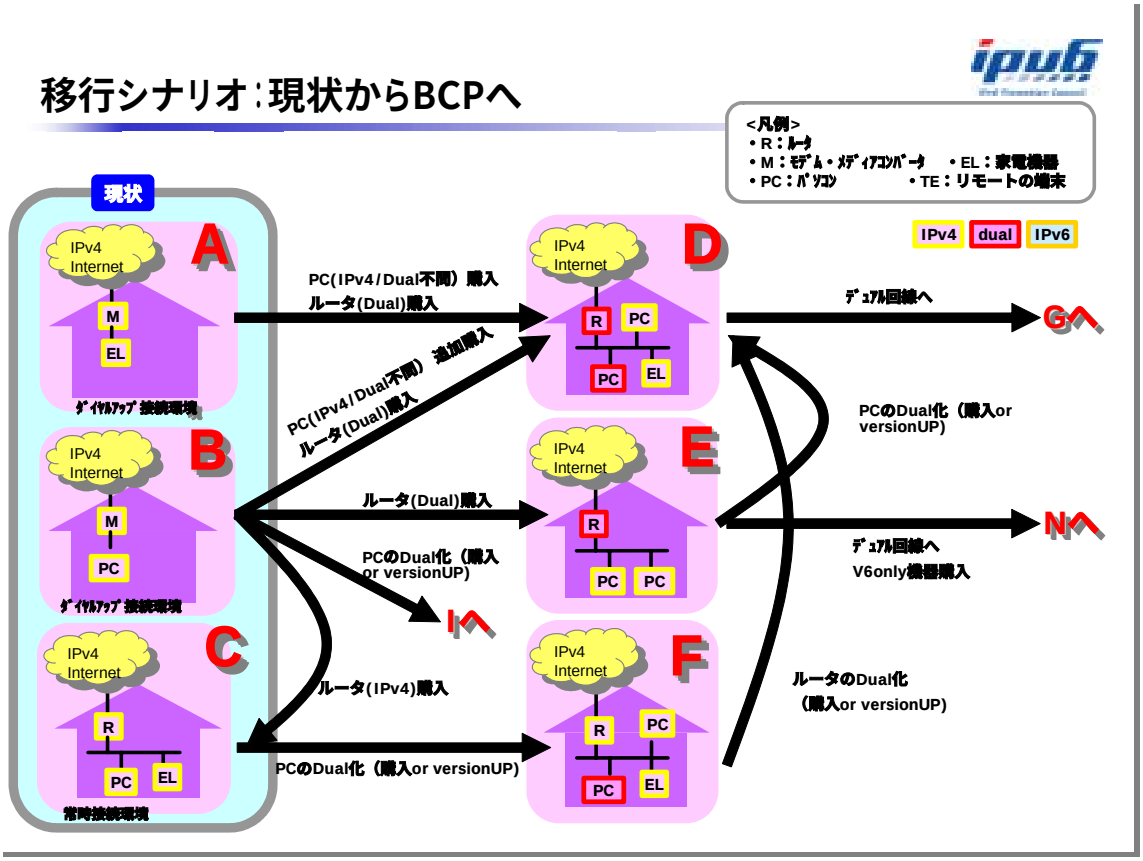
・ルータ接続による複数機器接続
・モデム（ダイアルアップ/ADSL モデム/メディアコンバータ）接続による端末１台のみの接続（ブリッジ接続）
・ネットワーク・機器なし

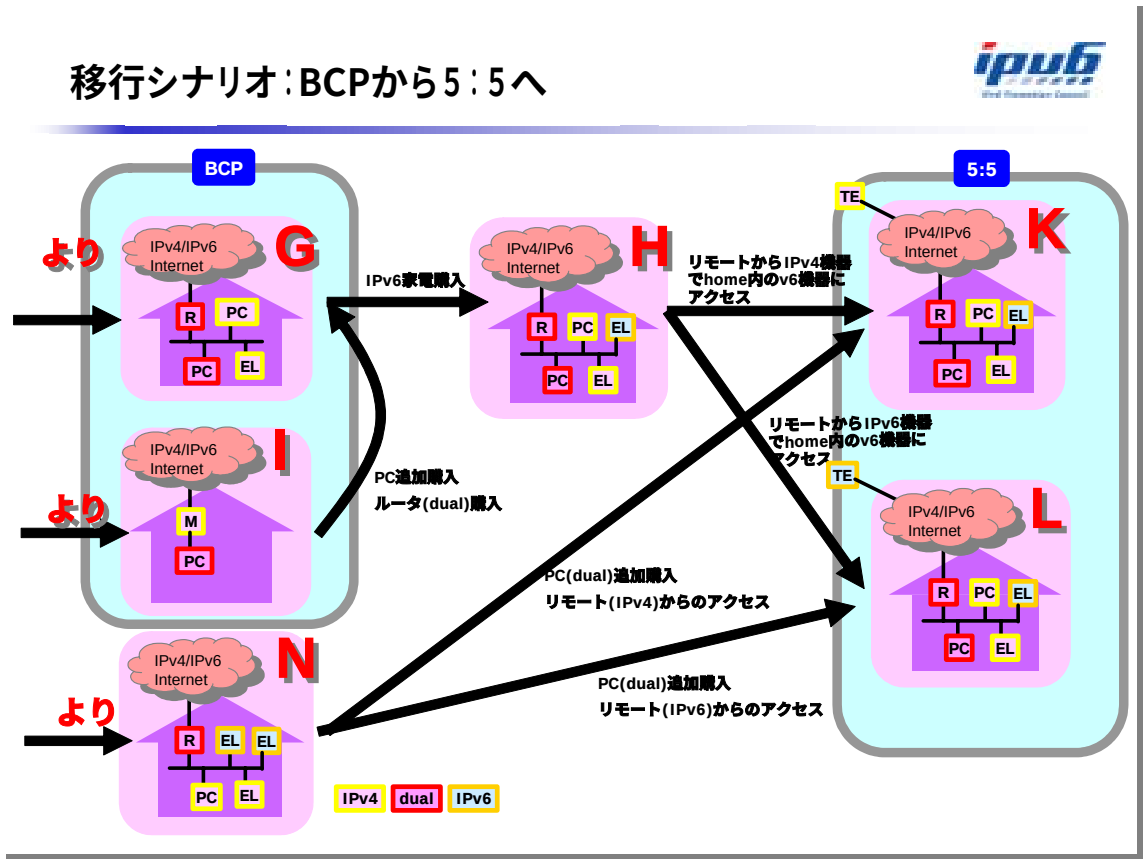
そして基本的には PC、Non PC 機器混在状況での IPv6 移行のシナリオを考えます。SOHO セグメントと共通の課題も多数ありますが、Non PC 機器を中心とした利用形態は家庭に特徴的です。現状、BCP、5 対 5 の状態における家庭のモデルを想定し、そのモデル間の差分を明確にすることで、移行における課題を整理します。

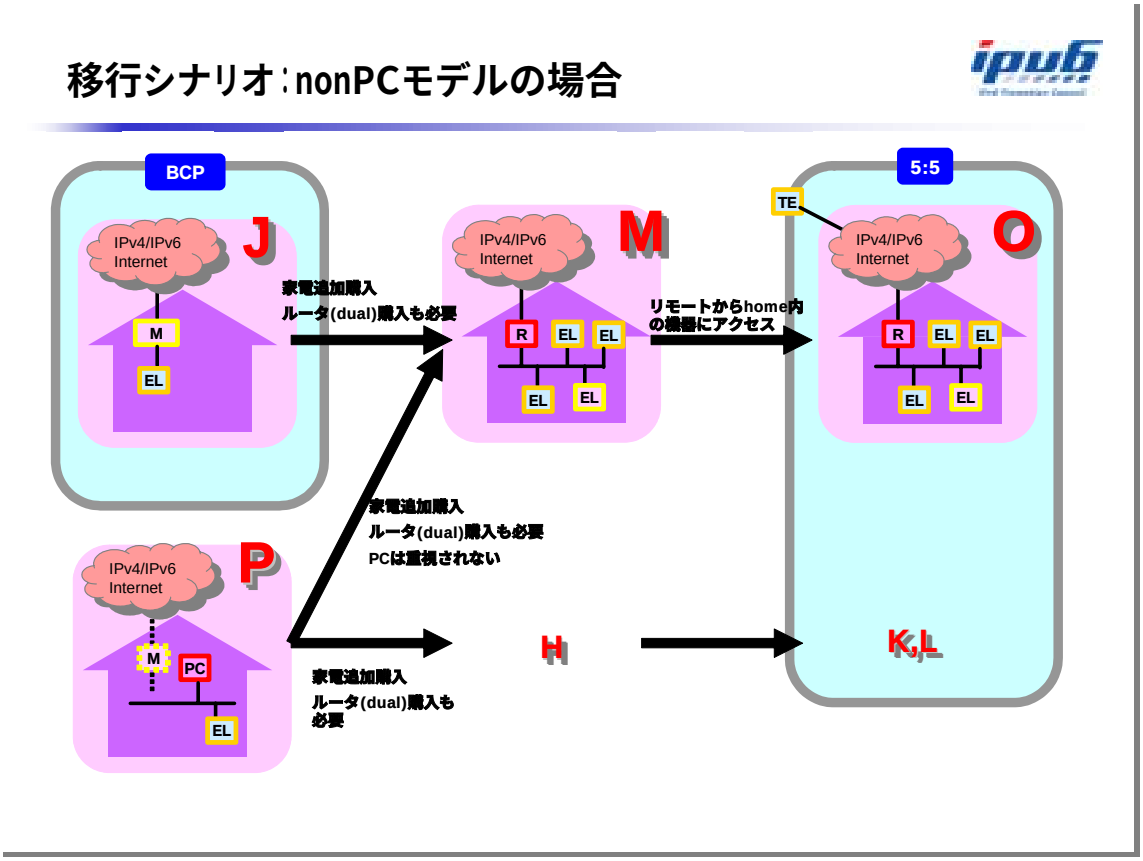
移行イメージは、全体的には以下の図に示す 3 つの移行シナリオとして表現することができます。これらのシナリオで、すべての考え得るモデルを網羅しているわけではありませんし、途中段階を順に経過する必要はありません。

しかし、基本的には、モデル A・B・C（現状）から D を経て、モデル G（BCP）経由でモデル K・L（5:5）へ向かうのが本流のシナリオと考えられます。ただし、これは SOHO セグメントや一般的な IPv6 への移行における課題と大差はありません。

家庭セグメントで考慮が必要な本流外シナリオとしては、まず、家電やゲーム機など、PC を持たないような家庭が、J→M→O という形で移行するシナリオが考えられます。また、宅内だけでネットワーク化する場合からの発展としては、P→ {M,H} → {K,L,O} が考えられます。





## ■各モデルの想定

各想定モデルについては、以下の項目で定義します。

・構成（ホームネットワーク内の機器とインターネットとの接続点）
・利用アプリ（家庭で使用されるアプリケーション）
・アドレス体系（割り当てられるアドレスと割り当てるアドレス）
・ネーミング（クエリ・登録の方法）
・セキュリティ対策（暗号化・不正アクセス対応・ウィルス対策・DoS 対策）
・設定方法（機器への設定方法）

### (1) モデルの想定：現状


家庭の現状としては、以下の 3 つのモデルが想定できます。

A：ダイアルアップ環境：モデル＋Non PC（ゲーム機など）
B：ダイアルアップ環境：モデル＋PC
C：常時接続環境：ルータ＋家庭内 LAN を構築

A と B におけるモデムには、ルータ機能を持たないブリッジ相当のモデム・メディアコンバータ等を含みます。

## モデルAの特徴

| | | |
|---|---|---|
| モデル | | A ：単機能モデル |
| 説明 | | 宅内に機器が1台 |
| 構成 | ネットワークとの境界 | モデムやMediaConverter(ブリッジ接続) |
| | 接続機器 | ゲーム機・nonPC機器 (AV機器・IPカメラ・IP電話など) |
| 利用アプリ | | ネットゲーム、リモート (携帯) からのVTR録画予約 |
| アドレス | インターネット側 | DHCP・PPPによるグローバルIP |
| | ローカル側 | --- |
| ネーミング | クエリ | (内→外) ISPより指定のDNSサーバ<br>(外→内) DDNSサービスやベンダー提供の専用サーバの利用 |
| | 登録 | 外部向け：DDNSやベンダー提供の専用サーバ |
| セキュリティ対策 | 暗号化 | 機器・アプリで個別に対応 |
| | 不正アクセス対応 | 同上 |
| | ウィルス対策 | 同上 |
| | DoS対策 | 同上 |
| 設定方法 | | なし |
| その他 | | |

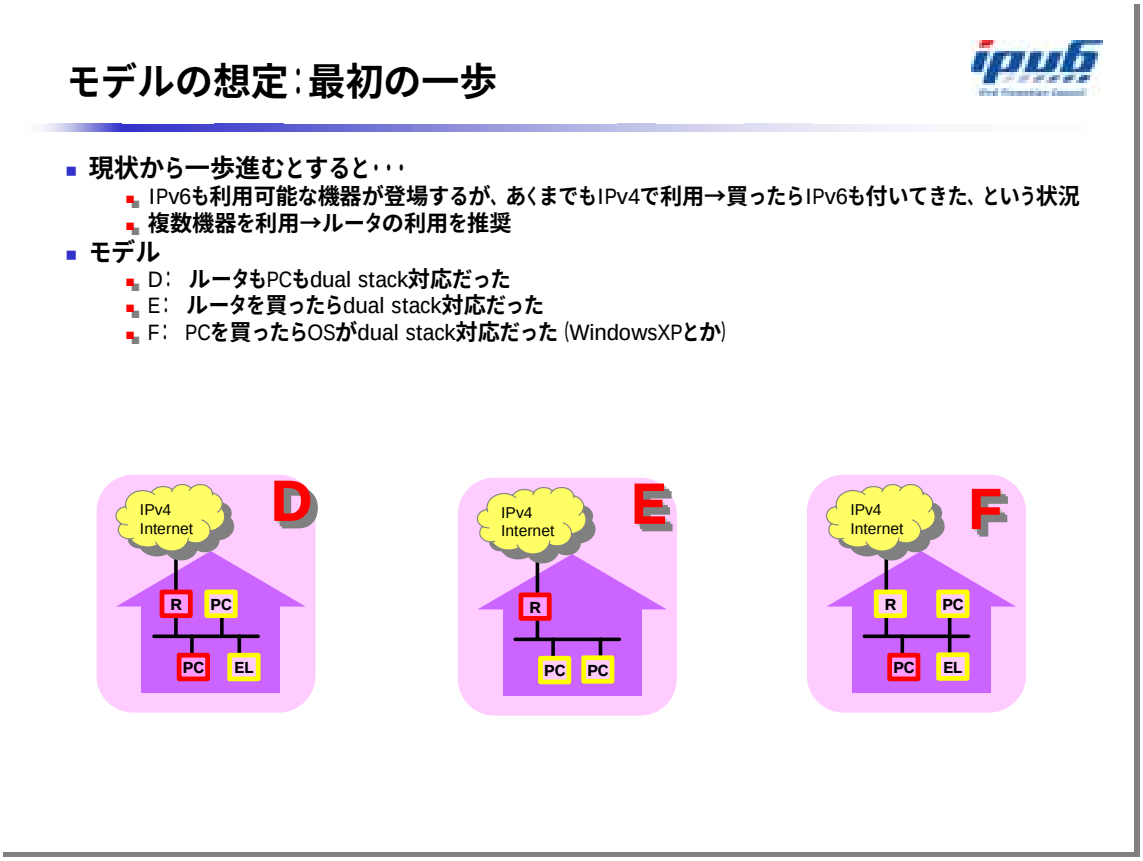
## モデルBの特徴

| | | |
|---|---|---|
| モデル | | B ：PCのみモデル |
| 説明 | | 宅内にPCが1台 |
| 構成 | ネットワークとの境界 | モデムやMC(ブリッジ接続) |
| | 接続機器 | PC |
| 利用アプリ | | Mail、WEB、ネットゲーム、会社のイントラと接続 |
| アドレス | インターネット側 | DHCP・PPPによるグローバルIP |
| | ローカル側 | --- |
| ネーミング | クエリ | (内→外) ISPより指定のDNSサーバ<br>(外→内) DDNSサービスやベンダー提供の専用サーバの利用 |
| | 登録 | 外部向け：DDNSやベンダー提供の専用サーバ |
| セキュリティ対策 | 暗号化 | 機器・アプリで個別に対応 |
| | 不正アクセス対応 | パーソナルファイアウォール |
| | ウィルス対策 | ウィルスチェッカー、ISPのサービス |
| | DoS対策 | パーソナルファイアウォール |
| 設定方法 | | Windowsアプリ、アプリごとの固有の設定方法、自動設定・更新 |
| その他 | | |

# モデルCの特徴

| | | |
|---|---|---|
| モデル | | C ：IPv4によるネットワーク |
| 説明 | | 宅内にPC/機器が複数台 |
| 構成 | ネットワークとの境界 | ルータ接続 |
| | 接続機器 | PC・ゲーム機・nonPC機器（AV・家電機器、IPカメラ、IP電話） |
| 利用アプリ | | Mail、WEB、ネットゲーム、会社のイントラと接続 |
| アドレス | インターネット側 | DHCP・PPPによるグローバルIP（ほぼ固定） |
| | ローカル側 | DHCP |
| ネーミング | クエリ | （内→外）ISPより指定のDNSサーバ、宅内向けにルータで中継<br>（外→内） DDNSサービスやベンダー提供の専用サーバの利用<br>ルータを越えるには設定が必要<br>（内→内）NETBIOS |
| | 登録 | 外部向け：DDNSやベンダー提供の専用サーバの利用 |
| セキュリティ対策 | 暗号化 | ルータ（PPTP、Ipsec：終端orスルー）<br>機器・アプリで個別に対応 |
| | 不正アクセス対応 | ルータで対応、パーソナルファイアウォール |
| | ウィルス対策 | ウィルスチェッカー、ISPのサービス |
| | DoS対策 | ルータで対応、パーソナルファイアウォール |
| 設定方法 | | Windowsアプリ、アプリごとの固有の設定方法、自動設定・更新 |
| その他 | | |

## (2) モデルの想定：最初の一歩




前述の 3 つの現状モデルから一歩進んだ形態としては、IPv6 も利用可能な機器が登場し、買ったらたまたま IPv6 も付いてきたが、あくまでも IPv4 で利用する、という状況が考えられます。ダイヤルアップユーザの間では、複数機器を利用する場合にはルータの利用が進み、このルータが IPv6 にも対応しているというケースが考えられるようになっていきます。この段階では IPv6 機能が家庭内に入ってくるということだけであり、必ずしも IPv6 が使われるということを意味していません。

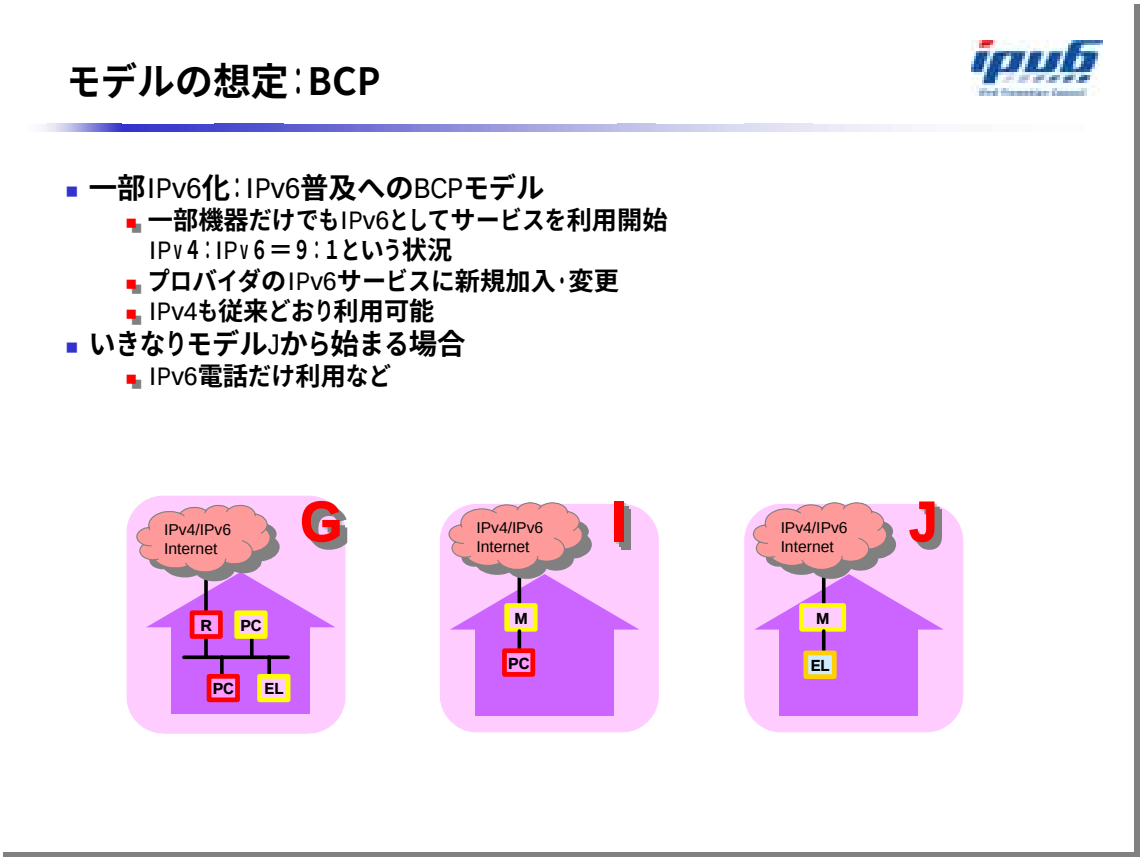
D： ルータも PC もデュアルスタック対応だった
E： ルータを買ったらデュアルスタック対応だった
F： PC を買ったら OS がデュアルスタック対応だった（Windows XP など）

# モデルDの特徴

**モデルE/Fについては基本的にモデルDと同じなので省略**

| | | |
|---|---|---|
| モデル | | D ：ルータ・PCはdualだがあくまでIPv4で利用 |
| 説明 | | 宅内にPC/機器が複数台 |
| 構成 | ネットワークとの境界 | ルータ接続 |
| | 接続機器 | PC・ゲーム機・nonPC機器（AV・家電機器、IPカメラ、IP電話） |
| 利用アプリ | | Mail、WEB、ネットゲーム、会社のイントラと接続、リモートからのVTR予約録画 |
| アドレス | インターネット側 | DHCP・PPPによるグローバルIP（ほぼ固定） |
| | ローカル側 | DHCP |
| ネーミング | クエリ | モデルCと同じ |
| | 登録 | モデルCと同じ |
| セキュリティ対策 | 暗号化 | ルータ（PPTP、Ipsec：終端orスルー）<br>機器・アプリで個別に対応 |
| | 不正アクセス対応 | ルータで対応、パーソナルファイアウォール |
| | ウィルス対策 | ウィルスチェッカー、ISPのサービス |
| | DoS対策 | ルータで対応、パーソナルファイアウォール |
| 設定方法 | | Windowsアプリ、アプリごと固有の設定方法、自動設定・更新 |
| その他 | | |

## (3) モデルの想定：BCP




次に、IPv6 における BCP（今すぐできること）ですが、この段階では、一部機器だけでも IPv6 としてサービスを利用開始することになります。IPv4 対 IPv6 は 9 対 1 という状況です。この時点で、IPv6 サービスを持つプロバイダに新規加入するか、既存プロバイダの IPv6 サービスへの変更が行なわれます。IPv4 も従来どおり利用可能です。一部では、IP 電話利用だけのためにインターネット接続を始めることが考えられ、この電話が IPv6 電話だったというケースが想定できます。この場合は、モデル J から始まることになります。

## モデルGの特徴

（IPv4部分についてはモデルC/Dと同じ）

| | | |
|---|---|---|
| モデル | | G ：PCだけIPv6利用、他はIPv4によるネットワーク |
| 説明 | | 宅内にPC/機器が複数台、一部PCはdual |
| 構成 | ネットワークとの境界 | ルータ(dual)接続 |
| | 接続機器 | PC・ゲーム機・nonPC機器（AV・家電機器、IPカメラ、IP電話） |
| 利用アプリ | | WEB、会社のイントラと接続？ |
| アドレス | インターネット側 | /48/64prefix、DHCPv6、6to4自動生成、configured、DTCP |
| | ローカル側 | RAでprefixを通知、リンクローカル |
| ネーミング | クエリ | 現状、WindowsXP-IPv6では不具合あり |
| | 登録 | |
| セキュリティ対策 | 暗号化 | ルータ、WIndowsXP（null暗号のIpsec） |
| | 不正アクセス対応 | ルータでパケットフィルタ。SPI<br>WindowsXP標準対応、パーソナルファイアウォールのv6化まだ |
| | ウィルス対策 | ウィルスチェッカー |
| | DoS対策 | 特になし |
| 設定方法 | | Windowsアプリ、アプリごと固有の設定方法、自動設定・更新 |
| その他 | | |

## モデルIの特徴

| | | |
|---|---|---|
| モデル | | I：Bの状況でとりあえずPCがdual対応のものに置き換わった |
| 説明 | | 宅内にPC/機器が1台、PCはdual |
| 構成 | ネットワークとの境界 | モデムorMC(ブリッジ接続) |
| | 接続機器 | PC |
| 利用アプリ | | インターネット、Closedネットワーク（Flet'sスクエアなど）と接続<br>WEB、会社のイントラと接続？ |
| アドレス | インターネット側 | (IPv4)DHCPかPPPでグローバルIPアドレスをもらう、1個 |
| | ローカル側 | (IPv6)RAでprefixを通知、リンクローカル |
| ネーミング | クエリ | ISPより指定のDNSサーバ、外部からはDDNS利用 |
| | 登録 | 外部向け：DDNS |
| セキュリティ対策 | 暗号化 | WIndowsXP（null暗号のIpsec） |
| | 不正アクセス対応 | WindowsXP標準対応、パーソナルファイアウォールのv6化必要 |
| | ウィルス対策 | ウィルスチェッカーのv6化必要、ISPで対応 |
| | DoS対策 | パーソナルファイアウォールで対応 |
| 設定方法 | | Windowsアプリ、アプリごと固有の設定方法、自動設定・更新 |
| その他 | | 使用したいアプリがv6only対応の場合に意味を持つモデル<br>そうでない場合はv4環境のみ使用され、ユーザにv6は意識されないのでは |

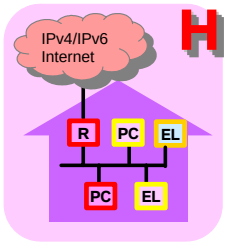
# モデルJの特徴

| | | |
|---|---|---|
| モデル | | J:家電お任せパック？ |
| 説明 | | 宅内にv6家電機器が1台 |
| 構成 | ネットワークとの境界 | モデムorMC(ブリッジ接続) |
| | 接続機器 | v6only家電・IP電話 |
| 利用アプリ | | 電話、ビデオ予約 |
| アドレス | インターネット側 | - |
| | ローカル側 | RAでprefixを通知 (認証が入るとRAできない)<br>リンクローカル |
| ネーミング | クエリ | 外部向け：DDNS、電話ならSIPサーバ、ベンダー提供の専用ネームサーバ |
| | 登録 | |
| セキュリティ対策 | 暗号化 | xSPまかせ。End機器では暗号化チップの搭載は可能か？ |
| | 不正アクセス対応 | |
| | ウィルス対策 | |
| | DoS対策 | |
| 設定方法 | | Windowsアプリ、アプリごと固有の設定方法、自動設定・更新 |
| その他 | | 家電とセットでxSPのサービスとして、電話・ビデオ予約等を利用<br>xSPのサービスとしてセキュリティ、エンド機器へのアドレッシング |

## (4) モデルの想定：５：５夜明け前

### モデルの想定：5：5夜明け前

- BCPよりさらに1歩進んでみる
  - IPv6しか話さない機器が登場
  - しかもv4機器とやり取りもあり得る
  - トランスレータ機能が必要



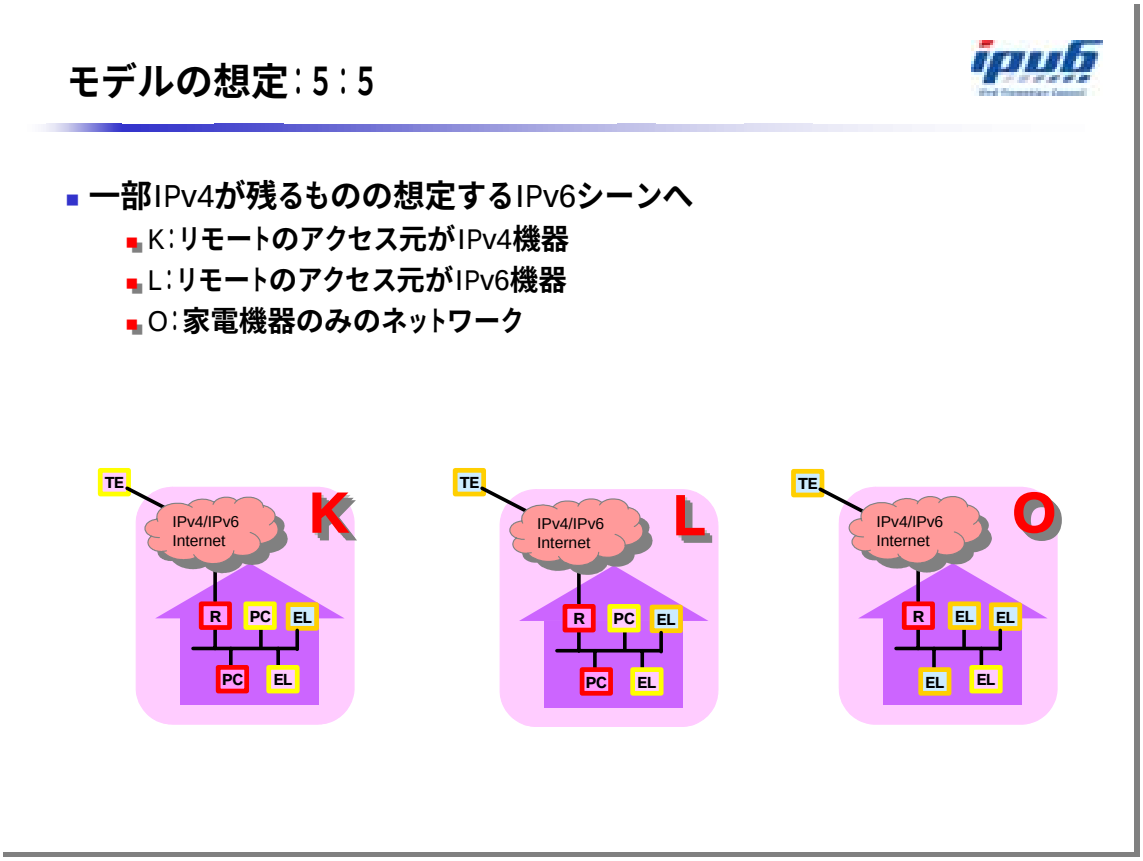

5 対 5 の環境に至る前に、IP 電話機など、IPv6 しか話さないものの、IPv4 とのやり取りも必要な機器が登場する可能性もあります。その際には、この 2 つのプロトコルの間の変換を行なう機能がどこかに置かれる必要があります。

# モデルHの特徴

## （IPv4部分についてはモデルC/Dと同じ）

| | | |
|---|---|---|
| モデル | | H ：Gも状況にIPv6だけを話す機器がきた |
| 説明 | | 宅内にPC/機器が複数台、一部PCはdual、一部はv6only |
| 構成 | ネットワークとの境界 | ルータ(dual)接続 |
| | 接続機器 | PC・ゲーム機・nonPC機器（AV・家電機器、IPカメラ、IP電話） |
| 利用アプリ | | WEB、会社のイントラと接続、宅内でv6機器同士の通信 |
| アドレス | インターネット側 | /48/64prefix、DHCPv6、6to4自動生成、configured、DTCP |
| | ローカル側 | RAでprefixを通知、リンクローカル |
| ネーミング | クエリ | （内→内）DNS-relay、個々にDDNS登録、uPnP-v6<br>現状、WindowsXP-IPv6では不具合あり |
| | 登録 | |
| セキュリティ対策 | 暗号化 | ルータ、WIndowsXP（null暗号のIpsec） |
| | 不正アクセス対応 | ルータでパケットフィルタ。SPI<br>WindowsXP標準対応、パーソナルファイアウォールのv6化進展 |
| | ウィルス対策 | ウィルスチェッカー |
| | DoS対策 | 特になし |
| 設定方法 | | Windowsアプリ、アプリごと固有の設定方法、自動設定・更新 |
| その他 | | トランスレータの位置は検討必要 |

## (5) モデルの想定：５：５




5 対 5 では、一部 IPv4 の利用が残りますが、この文書の冒頭で想定した IPv6 利用シーンが実現します。以下の 3 通りが考えられます。

K：家庭へのリモートアクセスで、アクセス元が IPv4 機器
L：家庭へのリモートアクセスで、アクセス元が IPv6 機器
O：家電機器のみのネットワーク

## モデルKの特徴

| | | |
|---|---|---|
| モデル | | K　Hの状況＋リモートから宅内機器にアクセスするv4機器 |
| 説明 | | 宅内にPC/機器が複数台、一部PCはdual、一部はv6only<br>外部機器はv4 |
| 構成 | ネットワークとの境界 | ルータ(dual)接続 |
| | 接続機器 | PC・ゲーム機・nonPC機器（AV・家電機器、IPカメラ、IP電話）<br>V4外部機器（携帯電話、PC（PDA）） |
| 利用アプリ | | 携帯からのVTR予約、外部の機器で宅内カメラ映像見る |
| アドレス | インターネット側 | /48/64prefix、DHCPv6、6to4自動生成、configured、DTCP |
| | ローカル側 | RAでprefixを通知、リンクローカル |
| ネーミング | クエリ | Hと同様 |
| | 登録 | |
| セキュリティ対策 | 暗号化 | ルータ、WIndowsXP（null暗号のIpsec） |
| | 不正アクセス対応 | ルータでパケットフィルタ。SPI<br>WindowsXP標準対応、パーソナルファイアウォールのv6化まだ |
| | ウィルス対策 | ウィルスチェッカー、ISPの提供サービスの利用 |
| | DoS対策 | 特になし |
| 設定方法 | | Windowsアプリ、アプリごと固有の設定方法、自動設定・更新 |
| その他 | | トランスレータ機能はルータ上への実装を推奨<br>ルータまでIPv4で接続する場合は、ルータの詳細な設定が必要。 |

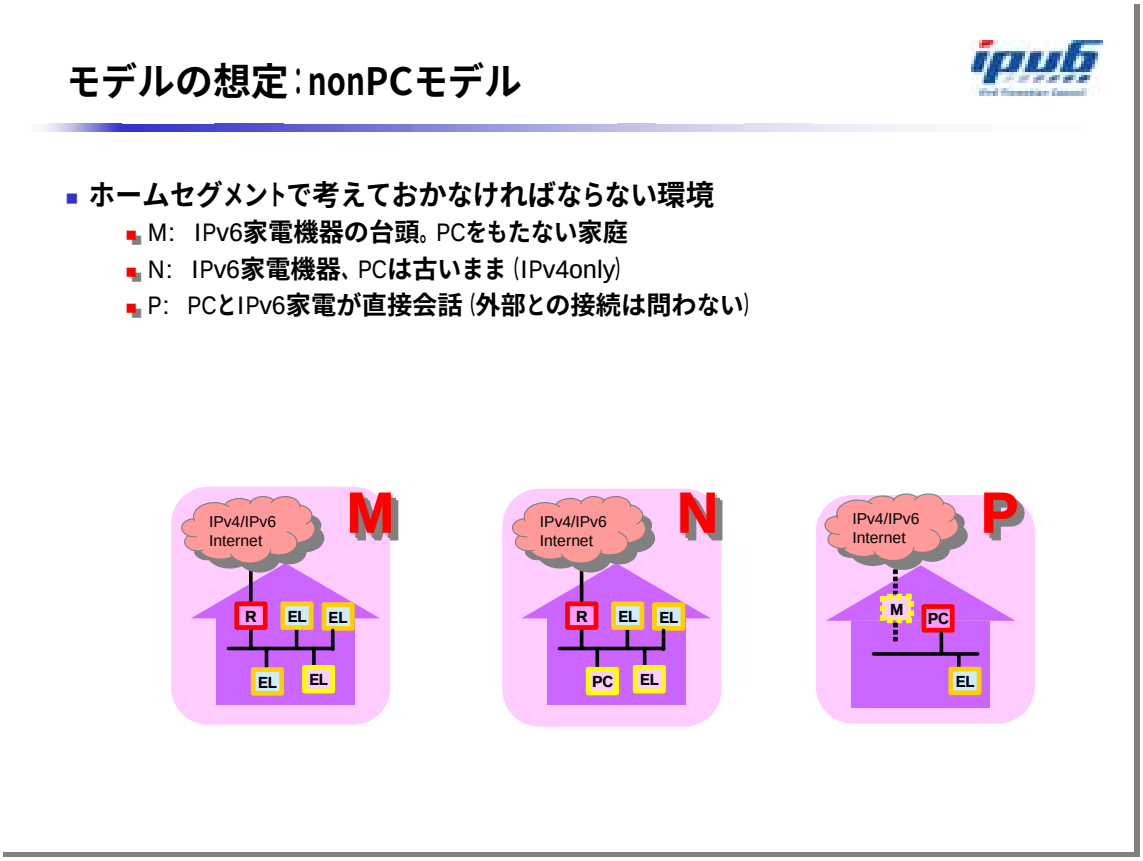
## モデルLの特徴　（基本的にはモデルKと同じ）

| | | |
|---|---|---|
| モデル | | L　Hの状況＋リモートから宅内機器にアクセスするv6機器 |
| 説明 | | 宅内にPC/機器が複数台、一部PCはdual、一部はv6only<br>外部機器はv6 |
| 構成 | ネットワークとの境界 | ルータ(dual)接続 |
| | 接続機器 | PC・ゲーム機・nonPC機器（AV・家電機器、IPカメラ、IP電話）<br>V6外部機器（PC（PDA）） |
| 利用アプリ | | 携帯からのVTR予約、外部の機器で宅内カメラ映像見る |
| アドレス | インターネット側 | /48/64prefix、DHCPv6、6to4自動生成、configured、DTCP |
| | ローカル側 | RAでprefixを通知、リンクローカル |
| ネーミング | クエリ | Hと同様 |
| | 登録 | |
| セキュリティ対策 | 暗号化 | ルータ、WIndowsXP（null暗号のIpsec） |
| | 不正アクセス対応 | ルータでパケットフィルタ。SPI<br>WindowsXP標準対応、パーソナルファイアウォールのv6化まだ |
| | ウィルス対策 | ウィルスチェッカー、ISPの提供サービスの利用 |
| | DoS対策 | 特になし |
| 設定方法 | | Windowsアプリ、アプリごと固有の設定方法、自動設定・更新 |
| その他 | | トランスレータ機能はルータ上への実装を推奨<br>宅内の機器一覧をどう取得するかがポイント |

## モデル O の特徴

モデル O は、基本的にはモデル K やモデル L と同じです。ただし、このモデルでは、Non PC 機器へ設定方法と内容が課題となります。名前の付け方や DNS 利用をどう設計するのが問題となります。たとえば、1 つの家庭内に、TV やビデオがそれぞれ複数台あった場合に、これらをどう区別できるかという問題です。

## (6) モデルの想定：nonPC モデル




家庭セグメントに特有の利用形態として、以下のような環境を考えておく必要があります。

M：もともと PC を持たない家庭で、IPv6 家電機器が利用されるようになる
N：PC は IPv4 利用のままだが、IPv6 家電機器が付け加わる
P：PC と IPv6 家電が直接会話する（外部との接続は問わない）

## モデルMの特徴

| | | |
|---|---|---|
| モデル | | M Jの状況から発展 |
| 説明 | | 宅内に機器が複数台、一部v4only、一部はv6only<br>ルータ(dual)が必要になる |
| 構成 | ネットワークとの境界 | ルータ(dual)接続 |
| | 接続機器 | ゲーム機・nonPC機器（AV・家電機器、IPカメラ、IP電話） |
| 利用アプリ | | TVとビデオ、TVで宅内カメラ映像見る |
| アドレス | インターネット側 | /48/64prefix、DHCPv6、6to4自動生成、configured、DTCP |
| | ローカル側 | RAでprefixを通知、リンクローカル |
| ネーミング | クエリ | uPnP |
| | 登録 | 宅内に閉じたDNSサーバ、命名方法 |
| セキュリティ対策 | 暗号化 | ルータ。End機器によっては対応 |
| | 不正アクセス対応 | ルータでパケットフィルタ。SPI<br>End機器では特になし（ルータに期待） |
| | ウィルス対策 | ISPのサービス |
| | DoS対策 | End機器では特になし |
| 設定方法 | | PCなしなので、ルータの設定、機器の設定はTV等のブラウザで行う。（ブラウザによっては設定画面が乱れる・出ないことも） |
| その他 | | |

モデル N の特徴は、基本的には M と同じですが、PC が存在することにより、下記の点が異なります。

・PC 上のパーソナルファイアウォールによるセキュリティ対策が可能
・PC（のブラウザ）によるルータ・機器の設定が可能

# モデルPの特徴

| | | |
|---|---|---|
| モデル | | P 家庭内島モデル |
| 説明 | | 宅内でv6家電とPCでネットワーク |
| 構成 | ネットワークとの境界 | 特に意識しない |
| | 接続機器 | V6家電、PC(dual) |
| 利用アプリ | | 家電機器とPCが連携（ビデオ予約、録画、映像をPCにコピーして利用、PCで映像記録など） |
| アドレス | インターネット側 | - |
| | ローカル側 | リンクローカル |
| ネーミング | クエリ | uPnP、SLP、NIQ |
| | 登録 | 利用毎に見つける |
| セキュリティ対策 | 暗号化 | 特になし。無線利用ならWEP等 |
| | 不正アクセス対応 | 特になし |
| | ウィルス対策 | 特になし |
| | DoS対策 | 特になし |
| 設定方法 | | 設定はPCやTV等のブラウザで行う。（ブラウザによっては設定画面が乱れる・出ないことも） |
| その他 | | |

## ■現状から BCP への移行ポイント

現状から BCP へ移行する際に考慮すべき課題を以下に示します。

### (1) 構成

現状でダイヤルアップ環境の家庭は、できればルータ利用の形態へ誘導すべきです。

### (2) アプリケーション

BCP 段階では、魅力的な IPv6 アプリケーションの提供が望まれます。現状のアプリケーションのままでは、ユーザは IPv4 で満足しています。IPv6 オンリーの IP 電話などが普及すれば、弾みがつくかもしれません。少なくとも、現状の IPv4 アプリケーションは IPv4 のまま使われ続けると思われます。また、アドレスや名前の登録・利用に関わる問題をクリアする必要が生じます。

### (3) セキュリティ

暗号化(IPsec)はルータで実施することが考えられます。PC では、パーソナルファイアウォールの IPv6 対応が待たれます。

### (4) その他

non PC 機器への各種設定方法の確立と自動化が望まれます。

## ■nonPC での移行シナリオ

PC 以外の機器の IPv6 への移行を考えた場合の課題は、基本的にはこれまで述べた一般的な移行シナリオの場合と同一です。

nonPC 機器に特有の状況としては、以下の 2 つが指摘できます。

・nonPC 機器は一般に非力であるため、セキュリティ機能を実装しにくく、ルータに期待せざるをえない
・nonPC の端末やルータを設定するには、Web ブラウザを使うしかない

# 3. 5:5 に向かうための課題

## ■セキュリティ

家電などの家庭用機器では、自己責任による利用を基本とする PC に比べ、対象とするユーザや利用方法が大きく広がります。このため、セキュリティについても、踏み込んだ対策が必要となります。

### (1) 暗号化

通信データの暗号化については、ルータで IPsec を利用する、端末機器で対応する、アプリケーションレベルで個別に対応する、の 3 通りが考えられます。暗号化処理はハードウェアによる処理を進めることにより、技術的には対応可能ですが、鍵の設定・交換をどうするのかが課題です、自動設定ができるか、手動設定なのか、手動設定の場合はサービスマンが対応するのかなど、現実的な方法を選択する必要があります。

### (2) 不正アクセス対応

一般的な外部 DNS に登録されると、不正アクセスを受ける危険性が増大します。DNS 情報の管理方法は大きな課題です。IPv6 利用に当たっては、少なくとも家庭用ルータで適切なパケットフィルタリングを行なうことが必要です。USAGI では、Linux 上でのステートフルパケットインスペクションをサポートしつつあります。IPsec の利用では、データを暗号化したままルータを通過させなければならないため、端末レベルでの対応も必要です。現状では、市販パーソナルファイアウォール製品で IPv6 に対応しているものはありません。Windows XP では、IPv6 パーソナルファイアウォールを標準で搭載しています。しかし、多くの Non PC 機器は、PC とは違って自衛することができません。したがって、ルータに守ってもらう必要があります。

### (3) ウィルス対策

電子メールソフトについては、IPv4 でサポートされていることでもあり、当面 IPv6 化する必要性はありません。これについては、IPv6 でのサポート体制の確立待ちとなります。ただし、IPv6 の世界では、プッシュ型でウイルスソフトのパターンファイルを更新するという新たな可能性も生まれます（ユーザにとっては、勝手に更新されると困ることもあります）。

### (4) DoS 対策

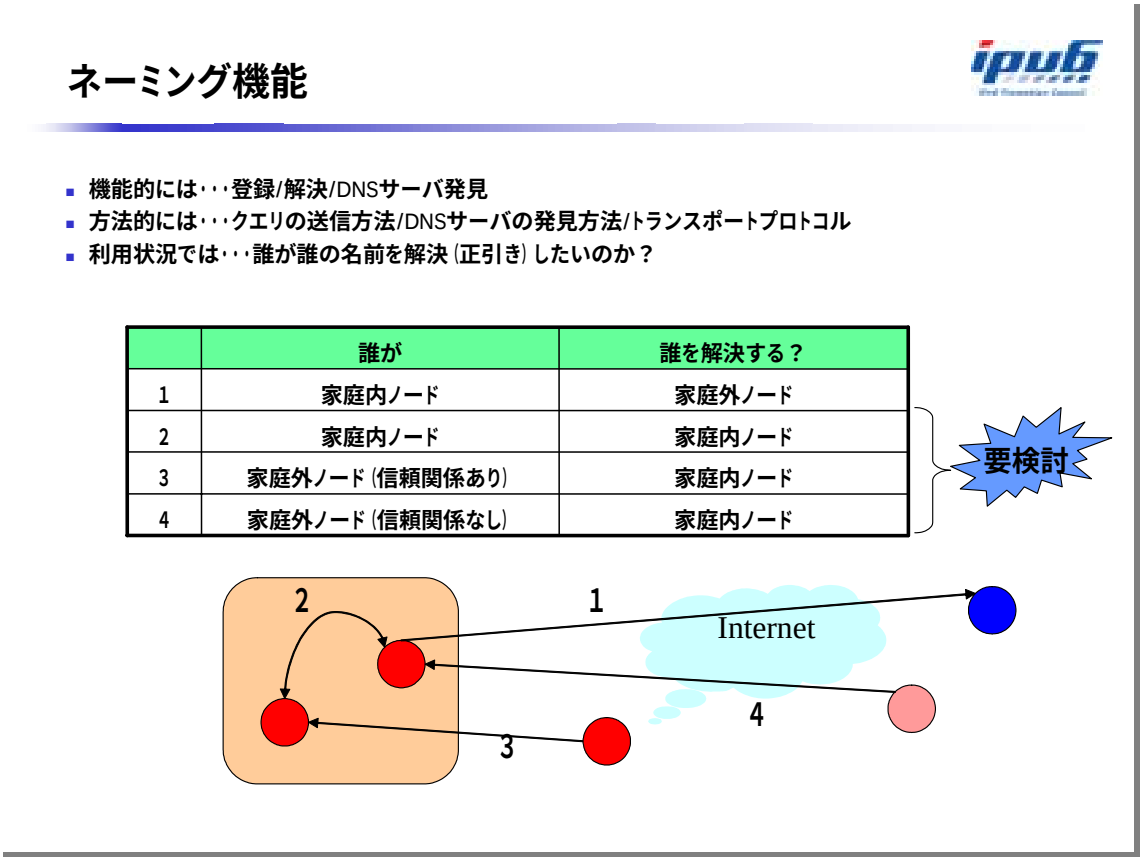
DoS 攻撃については、IPv4 でも IPv6 でも、基本的には防御する方法はありません。不正侵入検知システム（IDS）で検知、遮断することは可能ですが、ただしリソース消費やパフォーマンス低下まで回避することはできません。IPv4 スタックでは、コードの改良によって、DoS 攻撃によって簡単に落ちることはなくなってきました。しかし、IPv6 スタックならではの攻撃があるかもしれず、これについては未知数です。DoS 攻撃対策は、ISP での対応も求められます。Non PC 機器では、それ自体では有効な対策を期待することができないため、特にサービス側の対応が求められます。

## ■トランスレータ機能

IPv4 と IPv6 の間のトランスレータ機能が必要になるかどうかは、IPv6 オンリー機器が IPv4 オンリー機器と連携する必要性が生まれてくるかどうかに依存します。そして、こうしたトランスレータ機能の位置は、アプリケーションによって異なることが考えられます。

ISP やサービス業者など、家庭外に置かれることもあるでしょうし、ルータ上で稼働することも考えられます。この場合はアプリケーションに非依存となり、一番望ましい形態であるとも考えられます。もう 1 つの可能性としては、ホーム内の PC 上にある場合が考えられます。少なくとも家庭では、トランスレート用に専用機器が置かれることは考えられません。いずれにしろ、こうした機能では、電源が常に入っていることが望まれます。

# ■ネーミング機能




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。以下では、家庭内での名前解決、家庭外からの名前解決に分けて、課題や解決策を紹介します。

## (1) 家庭内での名前解決

家庭内端末が家庭内端末との通信する際の名前解決では、以下のような課題があります。

1. DNS サーバ発見プロセス
2. クエリ（問い合わせ）モデル
3. 機器情報の登録

### DNS 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 のエニー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。

ユニキャスト DNS サーバを利用する場合、Router Advertisement→DHCP→well-known マルチキャスト→手入力の順序で DNS 情報の自動設定を考えるのがよいと思われます（RA と DHCP は、実装サイズや運用状況によって、今後順序が入れ替わることも考えられます）。

**クエリ（問い合わせ）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。エニーキャスト 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。

推奨する方法は、ユニキャスト（自動設定）→エニーキャスト（well-known アドレス利用）→マルチキャスト（サーバなし）→ユニキャスト（手動設定）→ICMP Node Information Query の順序となります。

**機器情報の登録**

家庭で機器情報を登録する方法として、家庭内でも FQDN を使う方法や、利用者が適当に命名する方法があります。

家庭内で名前登録を行なう方法は、特にホームユーザには IP アドレスの入力や登録はきわめて負担が大きく、またそもそも表示や入力するインターフェースを持たない機器も想定されるため、困難です。そのため、DNS UPDATE や接続検出と自動登録など、自動登録手段が必須です。

この場合も、どの範囲に情報を公開するのか、家庭内における各個人のプライバシーの扱いをどうするか、さらに同一機種が複数存在する場合に区別できるような名前の付け方などの問題点を解決する必要があります。

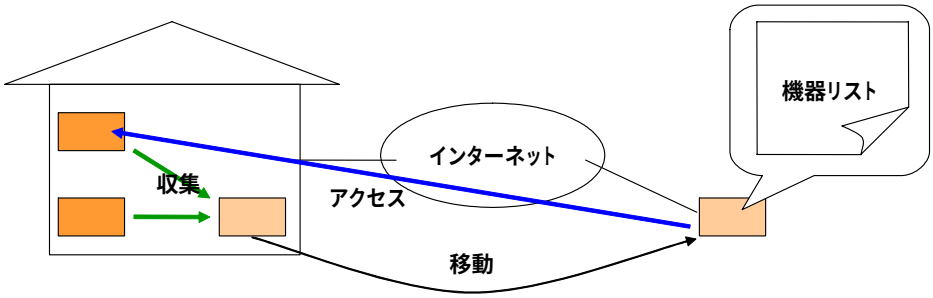
### (2) 家庭外からの名前解決

家庭外ノードが家庭内ノードを解決したい場合、登録はダイナミック 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。ISP が提供するサーバか、機器ベンダーが提供するサーバか、第三者が提供するサーバかを熟慮する必要があります。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。

## 事前収集モデル

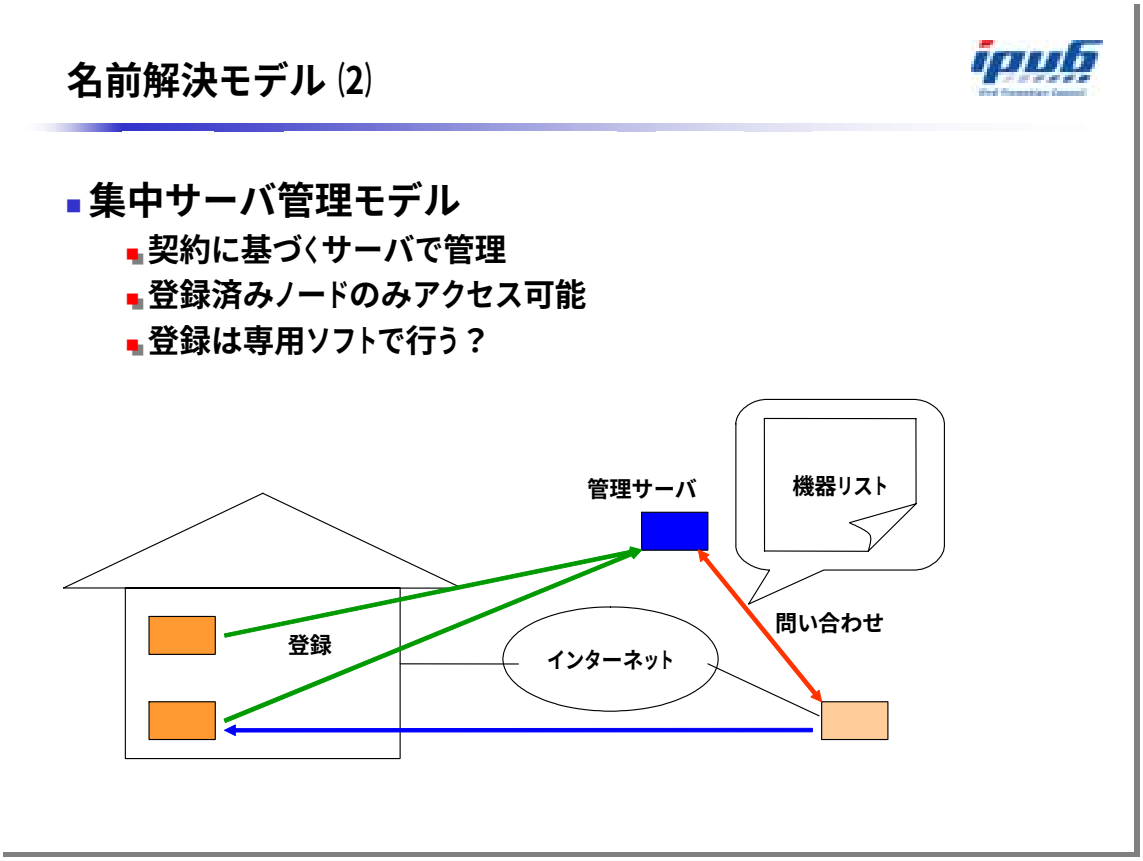
### 名前解決モデル (1)

- 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



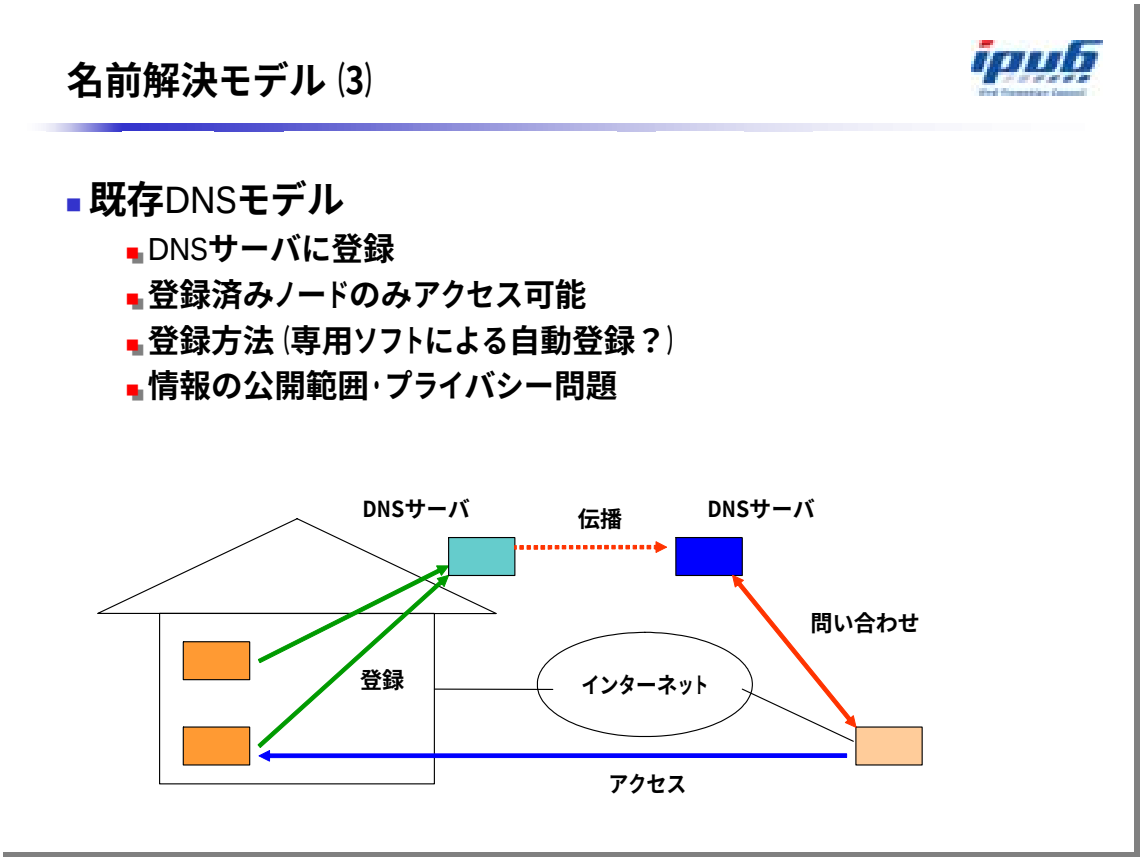

事前収集モデルでは、家庭の内外を移動する機器が、家庭内にいる間に、たとえば/etc/hostsの情報を取得しておき、家庭外に持ち出された場合にこれを使って名前解決をすることが考えられます。この場合、情報は持ち出された機器の内部にのみ存在するので安全です。しかし、機器毎の設定は必要となります。また、設定後(持ち出し後）のアドレス変更には追従できません。

## 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なうことになるかもしれません。

**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。

### (3) 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環境です。つまり 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。

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。

## ■ISP との接続

BCP の段階では、IPv6 サービスを使いたい機器（あるいはルータ）がトンネル接続するというケースも考えられます。静的トンネルや、DTCP、6to4、ISATAP、Teredo といった動的トンネルなど、方法はいろいろあるものの、それぞれが問題も抱えています。BCP としてまずはつなぐことが大事ですが、できるだけネイティブあるいはデュアルスタック接続に誘導したいところです。

## ■ISP への要望事項

家庭用ルータがある場合は、RA、DHCP、DTCP、ISATAP などさまざまなネットワーク構成方法があり、その方法により、アドレス付与の方法も異なってきます。配布するネットワークプレフィックスは/48、/64、/128 のどれなのかということも気になります。端末ベンダーからすれば、家庭セグメントの IPv6 移行については、このようなアドレスの払い出し方法を特定してほしいという要望があります。

例えば/48 を使う場合は、トランスレータトランスレータや DMZ 毎、また QoS のクラス毎にプリフィックスを割り当てたりする、などの設定方法も考えられます。

また、家庭用ルータがない場合、情報家電としては RA が望ましいといえます。セキュリティ面では課題が残るものの、特に追加の実装が不要という利点があります。

# 4. Tips & Tricks

## ■家庭セグメントでの全般的課題など

ソフトやファームウェアのバージョンアップは、特に IPv4 から IPv6 への移行期には頻繁に発生する可能性があります。これを、なるべくコストをかけずに実施する方法が必要となります。たとえば通常はプル型で行なうものの、セキュリティ問題発生時などはプッシュ型で実施するなどの使い分けも考えられます。

モバイル環境をどのようにサポートしていくか（家庭内の機器が家庭外のホットスポットに移動した場合など）についても検討が必要となります。

また、Non IP 機器（Echonet 機器や IEEE 1394 機器）の一部が IP（v6）機器へシフトしていくことが想定できます。

## ■nonPC での要検討事項

Non PC では、十分なリソース（CPU やメモリ）が期待できません。そのため、搭載できる機能に限界があります。まず、IPv4 と IPv6 の 2 つのスタックを搭載する余裕はありません。セキュリティ機能もなしか最小限となります（IPsec や暗号化チップはハード化されています）OS が TRON 系のものについては、スタックやネットワーク系ミドルウェア（DNS など）の IPv6 対応状況を確認する必要があります。また、RA はサポートすべきですが、それ以上のことはルータに期待することが考えられます。したがって、ユーザにはルータ利用を推奨しなければなりません。

Non PC 機器では、ほとんどの場合、設定の入力方法や設定内容の確認方法がないか、貧弱です。ユーザは「繋げば使える」という家電感覚を持っていますし、リモコンがあっても、2-3 行の液晶画面では設定しやすいとは言えません。したがって、できるだけ設定は自動化しなければなりません。また、家電機器は寿命が長いものですが、パッチ類の提供など、ベンダーとしていつまでサポートしていくのかという課題が残ります。

## ■PC なしでの設定方法

PC なしでの設定方法は大きな課題です。家庭への IPv6 普及を考えると、必ずしも PC を前提とすることはできません。これは IPv4 の世界でも同じですが。したがって、機器単独で設定できる方法が求められます。zero-conf などを利用してできるだけ自動設定できるようにするほか、TV（に搭載されるであろう）のブラウザ機能にも期待したいところです。携帯電話のブラウザ経由や IrDA 経由も可能かも知れません。ただし、利用を想定するブラウザでは必ず設定画面を表示できなければなりません。自動設定できない場合、別途設定サービスなどが必要となります。

# IPv6 移行ガイドライン（家庭セグメント）

平成 16 年 5 月発行

発　行　IPv6 普及・高度化推進協議会
連絡先　wg-dp-comment@v6pc.jp
URL　http://www.v6pc.jp/