

2005 年 IPv6 移行ガイドライン

家庭セグメント

2005 年 3 月

IPv6 普及・高度化推進協議会

移行 WG 家庭 SWG

目次

1.セグメントの特徴	4
全体像	4
家庭セグメントの特徴	5
プレイヤーの分類	5
エンド機器提供者	6
ネットワーク機器提供者	8
通信ネットワーク提供者	10
サービス提供者	11
現状の分析	20
統計情報	20
典型例	24
家庭内概略	25
2.ホームネットワークにおける移行シナリオ	27
ホームネットワークにおける移行シナリオの考え方	27
ホームネットワークにおける移行シナリオ (移行モデル概要)	27
ホームネットワークにおける移行シナリオ (シナリオ検討)	30
モデルの想定:現状	30
モデルの想定:最初の一步	35
モデルの想定:BCP	38
モデルの想定:IPv6 普及期夜明け前	42
モデルの想定:IPv6 普及期	46
モデルの想定:Non-PCモデル	49
現状からBCPへの移行ポイント	54
3.プレイヤーにおける移行シナリオ	56
サービス移行シナリオからの導入	56
遠隔メンテナンスシナリオ	56
ネットワークゲームシナリオ	61
各プレイヤーにおける移行シナリオ	66
プレイヤーにおけるシナリオ:エンド機器提供者	66
プレイヤーにおけるシナリオ:ネットワーク機器提供者	75
プレイヤーにおける移行シナリオ:通信ネットワーク提供者	80
プレイヤーにおける移行シナリオ:サービス提供者	80

4. IPv6 普及期に向けての課題	98
IPv6 普及期に向けての課題	98
トランスレータ機能	98
ネーミング	99

1.セグメントの特徴

全体像

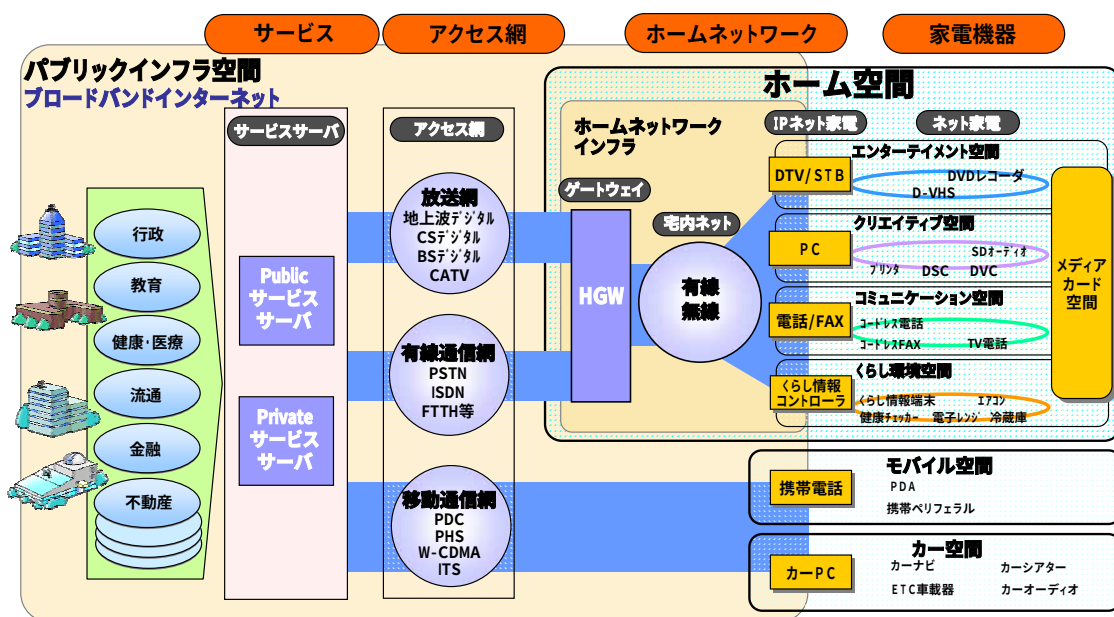
家庭のネットワークは、今後さまざまなメディア、プロトコル、機器により構成されていくことが予想されています。

インターネットを通じて提供されるサービスについては、公的なものも含めてますます多様化が進み、情報は地上波デジタル放送や衛星放送、ADSL や光ファイバー、無線アクセス技術、移動体通信などを通じて家庭に届けられるようになります。家庭内においても、場合によって有線、無線の複数の伝送技術が使い分けられ、セットップボックスや AV 家電、白物家電、PC、電話などを結びつけるようになっていきます。

1.1. 全体像



多様なメディア、プロトコル、機器により構成されることが予想されている



Oct 8, 2004

IPv6PC Transition WG Home SWG

6

より具体的には、インターネットアクセス網と家庭ネットワークの接続をホームゲートウェイ (家庭用ルータ) がつかさどります。家庭内のネットワーク機器は、エンターテインメント空間、クリエイティブ空間、コミュニケーション空間、くらし環境空間と、目的や接続機器によって分類され、各空間を構成する各機器群内で各種プロトコル (IEEE1394・USB・ECHONET など) が利用されること

になります。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) が存在する場合が出てきます。当初は、ネットワークに対応していても IP 以外のプロトコルを使うものが多いかもしれませんが、将来的には、non-IP 機器の IP 化が進んでいくことが考えられます。

家庭セグメントの特徴

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) が増加していくことが考えられます。

・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ません。デフォルト、あるいは一度設定したままで使い続けるケースが多いことが考えられます。さらに、今後登場してくる機器、特に家電は設定用のインタフェースを持たないことも考えられます。

・ISP の接続サービスを利用

家庭における ISP 接続形態は様々ですが、ホームネットワークは1サブネットが前提となります。有線 LAN、無線 LAN といった意味でのセグメント分割は行われていますが、全体は1つのサブネットとして ISP サービスを利用することになります。

本ガイドラインでは、家庭セグメントの移行を検討するにあたり、IP を終端する機器を対象とし、non-IP な機器・ネットワーク (ECHONET や IEEE1394 など) の IPv6 化はスコープ外とします。つまり、non-IP 機器は IP 機器を介して接続されるものと仮定します。

プレイヤーの分類

ここで、「プレイヤー」という言葉を導入することにします。プレイヤーとは、ここでは家庭で使用される製品、サービスの提供者を意味します。本ガイドラインの対象読者は何らかのプレイヤーです。具体的には、エンド機器提供者、ネットワーク機器提供者、通信ネットワーク提供者、サービス提供者などがこれにあたります。

エンド機器提供者

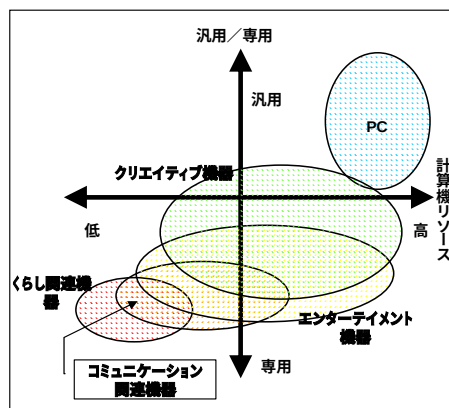
プレイヤーとしては、まずエンド機器の提供者がいます。エンド機器とは、最終的にネットワークにつながる末端の機器のことです。PC、ビデオレコーダーなどのエンターテインメント機器、デジタルカメラなどのクリエイティブ機器、エアコンなどのくらし関連機器、電話機などのコミュニケーション関連機器と、様々な種類の機器が家庭内ネットワーク上に混在することになります。

これらの機器は、まずネットワーク利用形態として、ユーザ主導で利用するものと、サービス提供者が利用するものがあります。計算機リソースの大小の点から見ると、小型組み込み機器、大型組み込み機器、PC に分けることができます。

1.3.1. プレイヤーの分類 (エンド機器提供者)



- エンド機器とは
 - PC
 - エンターテインメント機器
 - クリエイティブ機器
 - くらし関連機器
 - コミュニケーション関連機器
- 様々な種類の機器が混在する
 - ネットワーク利用形態
 - ユーザ主導で利用
 - サービス提供者が利用
 - 計算機リソース、機器の多様性
 - 小型組み込み機器
 - 大型組み込み機器
 - PC



PC

エンド機器の1つとしては、PCがあります。AT互換機やMacintoshなど、ハードウェアやOSは様々です。特徴としては、計算機資源量が豊富で、製品寿命は3年くらい、ホームネットワークの中心となりうる可能性を持っています。特に、既存PCの枠に収まらないPCの存在があります。「10feet UI」と呼ばれる、テレビのように多少離れてリモコンで操作するようなユーザーインターフェースを備えたPCも登場してきています。

PCは、ネットワークに対する要求の少ない機器です。つまり、PCはどのようなネットワークでも柔軟に対応可能です。

エンターテインメント機器

エンターテインメント機器としては、TV、HDDレコーダ／ビデオ、コンポ、STB、各種チューナー、ゲーム機などが挙げられます。

計算機資源量は製品によって様々であり、一概に表現することはできません。たとえばゲーム機は多く、TV等は少なくなっています。製品寿命は3～10年です。

ユーザーインタフェースを装備していることが多いのも特徴です。そのユーザーインタフェースは、入力系、表示系の両方を備えることが多く、ネットワーク経由で操作するためのユーザーインタフェースを備える場合もあります。

エンターテインメント機器では、コンテンツ管理に関する諸問題が大きく存在しており、利便性とのトレードオフを生んでいます。

ネットワークに対する要求としては、低遅延であること、適度な帯域があること(数 Mbps、MPEG2 クラスが配信できる程度、将来的には HD クラス)があります。

クリエイティブ機器

PC 周辺機器、デジカメ、デジタルビデオカメラなどをクリエイティブ機器として分類することができます。

計算機資源量は機器に依存しますが、製品寿命は3～5年が一般的です。大部分はPCとの接続、連携を前提にした機器設計が可能ですが、PCを利用しない動作をセールスポイントにすることもできます。

ユーザーインタフェースをどう設計するかは個々の製品のコンセプトに依存します。PCから操作できるようにする、単独で操作できるようにする(デジカメプリンタ連携、など)のどちらも考えられます。

ネットワークに対する要求としては、確実な接続性が求められます、また、適度な帯域があること(数 Mbps、やり取りするデータ量に依存)が必要です。

くらし関連機器

くらし関連機器には、白物家電や生活センサー(電気機器動作センサー、圧力センサー、光センサーなど)があります。特徴としては、計算機資源量に制限が大きく(KBの世界)、製品寿命は5年以上です。ユーザーインタフェースを持たないものがあり、あっても非常に貧弱(ボタン2つとLED1つ、など)です。

こうした機器については、利用者側は家電機器・部品という意識を持ち続ける可能性がありますし、販売側もこうした意識を持たせたいと考えています。「コンセントに電源コードを挿せば動く」という感覚です。

くらし関連機器には、空調機器、調理器具、給湯器具など誤動作が身体・生命に関わる機器があります。防犯センサーなど、犯罪に関連する機器もあります。また、建物に組み込まれて使用さ

れる場合もあります。

こうしたことから、ネットワークに対する要求としては、確実な接続性とデータの完全性確保が求められます。そして可能な場合には、通信の秘匿性が望まれます。

ネットワーク機器提供者

エンド機器提供者の次に、プレイヤーとして挙げられるのは、ネットワーク機器提供者です。ここに言うネットワーク機器とは、「家庭内ネットワークを構成するエンドノード以外の機器」を意味します。これらは、担当レイヤで細分化することができます。

レイヤ 2 までの機器としては、xDSL モデムや光メディアコンバータなどがあります。レイヤ 3 以上の機器にはルータなどがあります。そしてこれらを組み合わせた複合製品として、xDSL モデム + ルータ + IP 電話などがあります。

L2 以下のネットワーク機器

レイヤ 2 以下のネットワーク機器は、戸建用、集合住宅用、家庭内機器に分けることができます。

戸建用 (家庭と外部との接続機器) には、ADSL モデム、光メディアコンバータ、ケーブルモデム (ブリッジタイプ) などがあります。

特徴としては、アクセス事業者または ISP からレンタルするのが一般的であり、ADSL モデム、光メディアコンバータ、ケーブルモデムなどは相互接続の点から一般的に指定品となっています。これらの機器は、WAN メディア⇄Ethernet のメディア変換を行います。

集合住宅用の機器としては、イーサネットスイッチ (家庭間分割用)、VDSL コンセントレータ、Home PNA スイッチなどがあります。

特徴としては、複数のメディア、データリンク技術を結合する機能を備え、無線 LAN アクセスポイント (802.3, 802.11)、Bluetooth アクセスポイント (802.3, Bluetooth)、小電力無線 (小電力無線、802.3)、電灯線、電力線、TV アンテナ同軸ケーブルなどへの接続機能を提供していくことになると考えられます。建物に付帯設備として備わっている場合もあります。

複数の加入者回線を集約する一方、通常は加入者間で直接的な通信ができなくなっています。

また、家庭内の機器としては、イーサネットスイッチ (家庭内用)、無線 LAN アクセスポイント、Bluetooth アクセスポイントなどがあります。

レイヤ 3 以上のネットワーク機器

これには、ルータや認証サーバ (集合住宅内に設置) があります。

ルータでは、NAPT で最低限のセキュリティを確保しています。この場合、サーバ公開等をしなれば外部からの攻撃はある程度防御することができます。ルータがセキュリティ境界になるモデ

ルです。ファイアウォールや簡易 IDS などのセキュリティ機能が一般的に実装されてきている傾向にあります。一部では、ウィルスチェックやパターン更新を行う製品も登場しています。ただし、トロイの木馬やスパイウェアなどのペストやワームに対して無防備だといえます。

ルータの実装機能として、VPN、Mobile IP (ホームエージェント) の需要も高まっています。

IPv6 の実装については、まず 3 万円以上の価格帯のルータが先行しています。1万円以下の普及モデルでは、開発費も圧迫されており、具体的なメリットや利用シーンが確立しないと進みにくい状況にあります。

また、現状の IPv6 サービスでは事業者毎に方式が異なるため、ルータは事業者の指定品となっています。集合住宅内に設置される認証サーバの IPv6 化については、住民の総意が必要な場合があります。

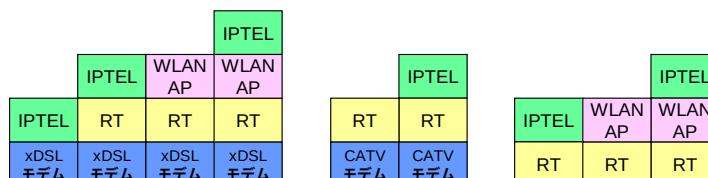
複合機器

複合機器は、多機能をシンプルな構成で提供できることから、広く利用されるようになってきています。利用者には比較的受け入れられやすい形態です。IPv6 普及の観点からは、こうした機器が IPv6 化することが望まれます。ただし、この種の機器では、モデムや IP 電話が搭載されている場合、接続性を保証するために、アクセス事業者または ISP の指定品であることが多いことが指摘できます。また、xDSL モデム+IP 電話など、特定のサービスに限定した製品も存在しています。このタイプの製品は、ホームネットワーク構成に大きく影響を与えます。

1.3.2. プレイヤーの分類 (ネットワーク機器提供者)

■ 複合機器

【例】



【特徴】

- 多機能かつシンプルな構成という需要から、一般的に利用されている
 - 比較的、利用者には受け入れられやすい
 - IPv6普及のためにIPv6化が期待される
- モデムやIP電話が搭載されている場合、アクセス事業者またはISPの指定品であることが多い (接続性保障のため)
- xDSLモデム+IP電話など、特定のサービスに限定した製品も存在する
- ホームネットワーク構成に大きく影響

通信ネットワーク提供者

さらにプレイヤーとしては、通信ネットワークの提供者がいます。ここでは、IPv6/IPv4 ネットワーク (IPv6/IPv4 インターネット接続) を提供している事業者を意味し、機能としては ISP コアネットワーク (IPv6/IPv4 インターネットへの接続機能を提供)、そしてアクセスネットワーク (ホームネットワーク～ISP コアネットワークの接続機能を提供) の 2 種類があります。アクセスネットワークの例としては、以下のようなものがあります。

xDSL、FTTH

アクセス事業者が提供することが多い (ISP が提供する例もある)

CATV

CATV 事業者が提供

無線 LAN

無線 LAN アクセス事業者、ISP が提供することが多い

携帯/PHS

携帯/PHS 通信キャリアが提供

IPv6 トンネル接続

ISP が提供することが多い

通常、ISP コアネットワークとアクセスネットワークは別に構築されることが多いですが、CATV インターネットサービスのよう、同一事業者が構築する場合があります。

アクセスネットワークには、サイト (site) 型とホスト (host) 型があります。

サイト型とは、家庭ネットワークがサイトとなっている形態のことです。家庭ネットワークにレイヤ 3 の CPE (ルータ) が存在します。

ホスト型は、レイヤ 3 的に家庭ネットワークからアクセスネットワークに直接接続される形態で、家庭ネットワークにレイヤ 2 CPE (モデム) が存在します。

通信サービス提供者は家庭に対し、通常次のようなネットワーク機能を提供しています。

アドレッシング

ホームネットワークに対してインターネット接続に必要なアドレスを配布する

ルーティング

IPv6、および IPv4 インターネット接続のためのパケットルーティングを行う

通常、ISP 側への固定デフォルトルーティング (ネットワーク機器にて標準設定 → 暗黙の了解)

マルチホーミングなどにより、上記の前提が崩れる場合もある

通信ネットワーク提供者は、ホームネットワークの形態に大きな影響を与えます。たとえば WAN 接続方法はサイト型かホスト型か、アドレス払い出し数は 1 つか複数か、アドレス種別はグローバルかプライベートか、同時接続数は 1 台限定か NAT 経由の複数台接続を受け付けるか、といった点を左右します。

さらに通信ネットワーク提供者は、機器開発にも影響を与えます。たとえば NAT Traversal の有無 (NAT を提供するか否か)、エンドノードのセキュリティ機構 (セキュリティ機構を提供するか否か) などを左右します。特にネットワーク機器 (CPE) が搭載する機能に大きな影響を与えます。

サービス提供者

上記のようなホームネットワークインフラの上で、各機器群に対し、様々なネットワークサービスの展開が考えられます。例としては以下のようなものが考えられます。

《PC》

旧来インターネットアプリケーション (Web, FTP, Mail, ...)

他の機器に対するサービスも利用可能

《エンターテインメント機器》

コンテンツ配信、ネットワークゲーム、ビデオ予約

《くらし機器》

ホームセキュリティ、くらし補助、福祉、遠隔メンテナンス

《コミュニケーション機器》

IP 電話、TV 電話

《クリエイティブ機器》

印刷、映像・音楽編集

こうした『サービス』とエンド機器は密接に関係しています。特定のサービスに必須なエンド機器が存在したり、サーバや家庭内端末との連携が前提となるアプリケーションやシステムが存在したりします。また、エンド機器提供者が行うサービスとエンド機器提供者以外が行うサービスが考えられます。これらサービスのネットワークへの要求は、サービス種別やその提供形態により様々です。ASP に対する共通サービス (他ポータルとの連携も B2B2C) もありえます。たとえば課金管理、ユーザ認証管理、セキュリティ管理、ジョブ管理などです。

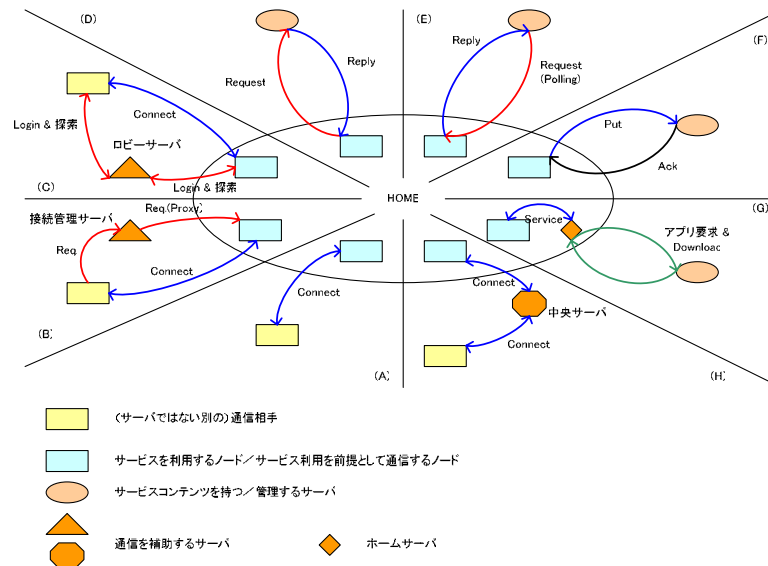
これらのサービスを通信形態によって分類すると、以下のようになります。

- (A) 完全 P2P 型
- (B) P2P+接続管理サーバ型
- (C) P2P+ロビーサーバ型
- (D) クライアント・サーバ型
- (E) クライアント・サーバ (ASP ポーリング) 型
- (F) クライアント・サーバ (クライアントポスト) 型
- (G) ホームサーバ型
- (H) 中央サーバ経由型

サービスを、その種別やネットワークへの要求などで分類する方法も考えられますが、多様化するサービスを網羅できないと判断し、ここでは通信形態による分類を行っています。

1.3.4. プレイヤーの分類 (サービス提供者)

■ サービスの分類 通信形態による分類 図解



Oct 8, 2004

IPv6PC Transition WG Home SWG

30

以下では、サービスの各種通信形態の詳細を、順に見ていくことにします。

(A) 完全 P2P 型

エンドノードが直接通信相手を見つけ、P2P 通信を行う通信形態で、通信相手の発見は DNS やサービス発見プロトコルなどを使用します。

利用例: 自律型ファイル交換ソフト、家庭内連携

サービス提供者の役割: アプリケーションソフトウェアの提供

トラフィック: 始点—P2P 参加ノード

終点—P2P 参加ノード

経路—直接通信

特徴: ノードに依存するが、サーバがないため一極集中にはならない

その他: NAT 裏の IPv4 ノードが通信するためにはポートフォワード、DMZ などの設定を必要とする

1.3.4. プレイヤーの分類 (サービス提供者)

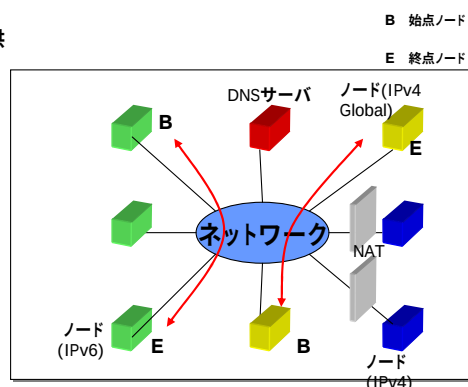
■ 通信形態の詳細

(A) 完全P2P型

直前のページに戻ります



- エンドノードが直接通信相手を見つけ、P2P通信を行う通信形態
 - 通信相手の発見はDNSやサービス発見プロトコルなどを使用する
- 利用例
 - 自律型ファイル交換ソフト
 - 家庭内連携
- サービス提供者の役割
 - アプリケーションソフトウェアの提供
- トラフィック
 - 始点 P2P参加ノード
 - 終点 P2P参加ノード
 - 経路 直接通信
 - 特徴
 - ノードに依存するが、サーバが無い場合極集中にはならない
- その他
 - NAT裏のIPv4ノードが通信するためにはポートフォワード、DMZなどの設定を必要とする



Oct 8, 2004

IPv6PC Transition WG Home SWG

31

(B) P2P+接続管理サーバ型

これはエンドノードが通信ポリシーや接続制限などを行う接続管理サーバを介して通信相手を発見し、P2P 通信を行う通信形態です。

利用例: IP 電話、接続管理された SIP ベースのアプリケーション

サービス提供者の役割: アプリケーションソフトウェアの提供、接続管理サーバの運用

トラフィック: 始点—P2P 参加ノード

終点—P2P 参加ノード

経路—初動通信はサーバ経由、通常通信は直接通信

特徴: ノード数が増えると管理サーバにトラフィックが集中する

その他: (A) と同様の NAT 問題があります。

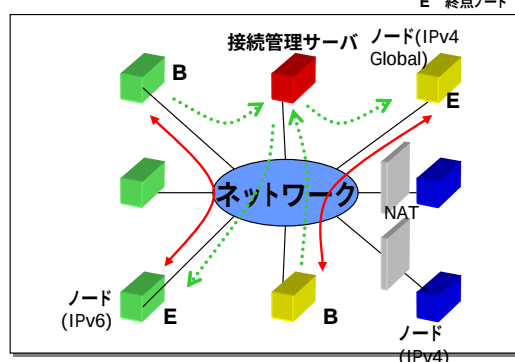
1.3.4. プレイヤーの分類 (サービス提供者)

■ 通信形態の詳細



(B) P2P+接続管理サーバ型

- エンドノードが通信ポリシーや接続制限などを行う接続管理サーバを介して通信相手を発見し、P2P通信を行う通信形態
- 利用例
 - IP電話
 - 接続管理されたSIPベースのアプリケーション
- サービス提供者の役割
 - アプリケーションソフトウェアの提供
 - 接続管理サーバの運用
- トラフィック
 - 始点 P2P参加ノード
 - 終点 P2P参加ノード
 - 経路 初動通信はサーバ経由
通常通信は直接通信
 - 特徴
 - ノード数が増えると管理サーバにトラフィックが集中する
- その他
 - NAT問題は同様



Oct 8, 2004

IPv6PC Transition WG Home SWG

32

(C) P2P+ロビーサーバ型

プレゼンス情報を保持するロビーサーバを介して通信相手を発見し、P2P通信を行う通信形態で、ポリシーの適用や接続制限を行わない点が(B)と異なります。

利用例: P2P型インターネットゲーム、放送型アプリケーション(放送局リストを起点としたP2Pの場合)

サービス提供者の役割: アプリケーションソフトウェアの提供、ロビーサーバの運用

トラフィック: 始点—P2P参加ノード

終点—P2P参加ノード

経路—初動通信はサーバ経由、通常通信は直接通信

特徴: (B)と同じ

その他: NAT問題は(A)と同様

1.3.4. プレイヤーの分類 (サービス提供者)

■ 通信形態の詳細



(C) P2P+ロビーサーバ型

- プレゼンス情報を保持するロビーサーバを介して通信相手を発見し、P2P通信を行う通信形態
 - ポリシの適用や接続制限を行わない点が(B)と異なる

■ 利用例

- P2P型インターネットゲーム
- 放送型アプリケーション (放送局リストを起点としたP2Pの場合)
- サービス提供者の役割

- アプリケーションソフトウェアの提供

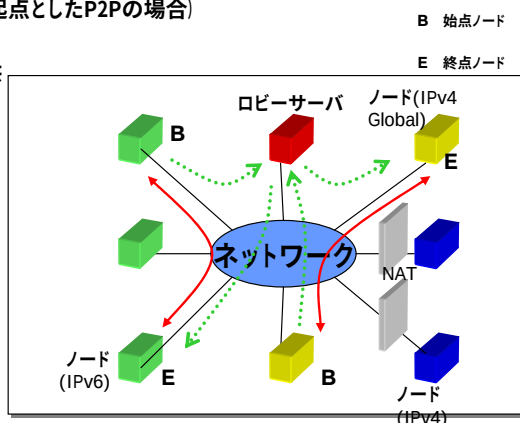
- ロビーサーバの運用

■ トラフィック

- 始点 P2P参加ノード
- 終点 P2P参加ノード
- 経路 初動通信はサーバ経由
通常通信は直接通信

- 特徴
 - (B)と同じ

- その他
 - NAT問題は同様



Oct 8, 2004

IPv6PC Transition WG Home SWG

33

(D) クライアント・サーバ型

クライアントがサーバから何らかの情報を取得することによって機能する通信形態です。

利用例: Web、FTP、Mail、など既存インターネットアプリケーション、VoD などの放送型アプリケーション、クライアント・サーバ型インスタントメッセージ、C/S 型インターネットゲーム (MMOG など)

サービス提供者の役割: アプリケーションソフトウェアの提供、サーバの運用

トラフィック: 始点—クライアント

終点—サーバ

経路—すべての通信はサーバに向かう

特徴: サーバにトラフィックが集中する

その他: NAT 裏からも利用可能

1.3.4. プレイヤーの分類 (サービス提供者)

■ 通信形態の詳細



(D) Client/Server型

- クライアントがサーバから何らかの情報を取得することによって機能する通信形態

■ 利用例

- Web、FTP、Mail、など既存インターネットアプリケーション
- VoDなどの放送型アプリケーション
- C/S型インスタントメッセージ、C/S型インターネットゲーム (MMOGなど)

■ サービス提供者の役割

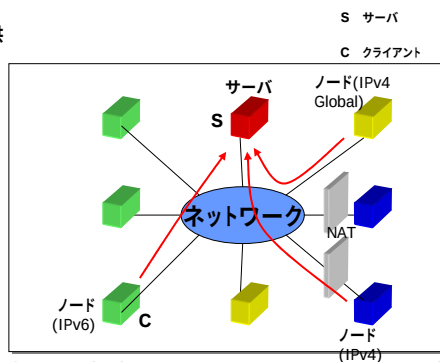
- アプリケーションソフトウェアの提供
- サーバの運用

■ トラフィック

- 始点 クライアント
- 終点 サーバ
- 経路 全ての通信はサーバに向かう
- 特徴
 - サーバにトラフィックが集中する

■ その他

- NAT裏からも利用可能



Oct 8, 2004

IPv6PC Transition WG Home SWG

34

(E) Client/Server (ASP ポーリング) 型

これは、ASP のクライアントが家庭内のサーバから何らかの情報を取得することによって機能する通信形態です。

利用例: テレメータリング、遠隔監視、遠隔メンテナンス (ASP からの定期的な動作確認)

サービス提供者の役割: 対応機器の販売、アプリケーションの提供、ASP 内ノードの運用、収集情報の整理・管理、など

トラフィック: 始点—ASP (クライアント)

終点—家庭内 (サーバ)

経路—すべての通信は ASP から開始される

特徴: ASP がトラフィックを制御可能

その他: NAT 裏へは到達できない

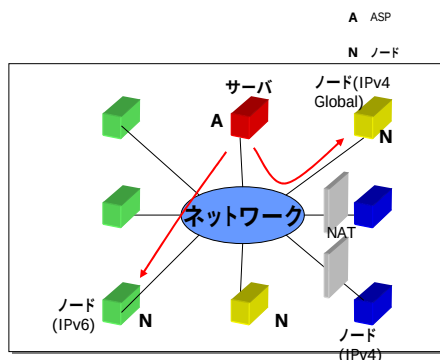
1.3.4. プレイヤーの分類 (サービス提供者)

■ 通信形態の詳細



(E) Client/Server (ASPポーリング) 型

- ASPのクライアントが家庭内のサーバから何らかの情報を取得することによって機能する通信形態
- 利用例
 - テレメータリング、遠隔監視
 - 遠隔メンテナンス (ASPからの定期的な動作確認)
- サービス提供者の役割
 - 対応機器の販売
 - アプリケーションの提供
 - ASP内ノードの運用、収集情報の整理・管理、など
- トラフィック
 - 始点 ASP (クライアント)
 - 終点 家庭内 (サーバ)
 - 経路 全ての通信はASPから開始される
 - 特徴
 - ASPがトラフィックを制御可能
- その他
 - NAT裏へは到達できない



Oct 8, 2004

IPv6PC Transition WG Home SWG

35

(F) クライアント・サーバ (クライアントポスト) 型

家庭内のクライアントから ASP のサーバに何らかの情報を通知することによって機能する通信形態です。クライアントからサーバに情報を通知する点が(D)と異なります。

利用例: 遠隔監視 (監視画像等の定期的なアップロード)、遠隔メンテナンス (センサーノードからの定期的な情報通知)、ホームセキュリティ (イベントに基づく情報通知)

サービス提供者の役割: 対応機器の販売、アプリケーションの提供、ASP 内ノードの運用、収集情報の整理・管理、など

トラフィック: 始点—家庭内

終点—ASP

経路—全通信は ASP に集中する

特徴: ASP が制御できない場合が多い (機器に依存)

その他: NAT 裏からも利用可能

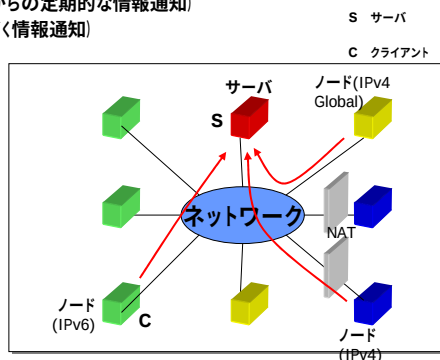
1.3.4. プレイヤーの分類 (サービス提供者)

■ 通信形態の詳細



(F) Client/Server (クライアントポスト) 型

- 家庭内のクライアントからASPのサーバに何らかの情報を通知することによって機能する通信形態
 - クライアントからサーバに情報を通知する点が(D)と異なる
- 利用例
 - 遠隔監視 (監視画像等の定期的なアップロード)
 - 遠隔メンテナンス (センサーノードからの定期的な情報通知)
 - ホームセキュリティ (イベントに基づく情報通知)
- サービス提供者の役割
 - 対応機器の販売
 - アプリケーションの提供
 - ASP内ノードの運用、収集情報の整理・管理、など
- トラフィック
 - 始点 家庭内 終点 ASP
 - 経路 全通信はASPに集中する
 - 特徴
 - ASPが制御できない場合が多い (機器に依存)
- その他 NAT裏からも利用可能



Oct 8, 2004

IPv6PC Transition WG Home SWG

36

(G) ホームサーバ型

ASP からのアプリケーションを、ダウンロードとそれが実行されて発生する家庭内通信により構成される通信形態で、(D)と(A)の複合モデルと見ることができます。

利用例: 現状では存在しない?

サービス提供者の役割: ダウンロードされるアプリケーションの提供、連携先ノードのアプリケーションの提供、(実行プラットフォームとしての) 対応機器の販売

トラフィック: 始点—家庭内 (ダウンロード時)

終点—ASP (ダウンロード時)

経路—ダウンロード時のみサーバに集中するが、通常は家庭内で閉じる

特徴: バージョンアップ時などにダウンロードが急激に集中する可能性がある

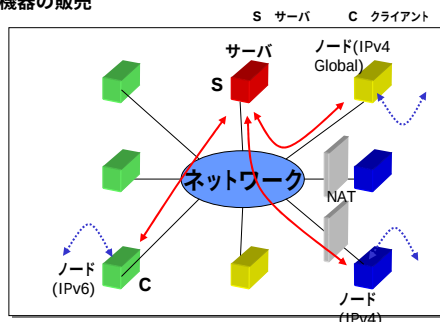
その他: NAT 裏からも利用可能

1.3.4. プレイヤーの分類 (サービス提供者)

■ 通信形態の詳細

(G) ホームサーバ型

- ASPからのアプリケーションをダウンロードとそれが実行されて発生する家庭内通信により構成される通信形態
 - (D)と(A)の複合モデルと見ることが出来る
- 利用例
 - 現状では存在しない？
- サービス提供者の役割
 - ダウンロードされるアプリケーションの提供、連携先ノードのアプリケーションの提供
 - (実行プラットフォームとしての) 対応機器の販売
- トラフィック
 - 始点 家庭内 (ダウンロード時)
 - 終点 ASP (ダウンロード時)
 - 経路 ダウンロード時のみサーバに集中するが、通常は家庭内で閉じる
 - 特徴
 - バージョンアップ時などにダウンロードが急激に集中する可能性がある
- その他 NAT裏からも利用可能



Oct 8, 2004

IPv6PC Transition WG Home SWG

37

(H) 中央サーバ経由型

すべての通信が中央サーバを経由して行う通信形態です。

利用例: 一部の遠隔アクセスサービス、ウィルスチェックなどの通信経路に対する付加機能の提供

サービス提供者の役割: アプリケーションソフトウェアの販売、サーバの運用

トラフィック: 始点—家庭内

終点—サーバ (本質的には対向ノード)

経路—全トラフィックが必ずサーバを経由する

特徴: 利用者数の増加に伴ってトラフィックが急激に増加する

その他: NAT 裏からも利用できる

現状の分析

統計情報

総務省の「インターネット接続サービスの利用者数等の推移 (平成 16 年8月末現在)」によると、現状の家庭におけるインターネット接続・利用状況は以下の通りです。

インターネットとの接続方法

ダイヤルアップ加入者数 約 1862 万契約

PC (モデム) より直接ダイヤルアップ (PSTN)

ダイヤルアップルータ (ISDN)

常時接続環境加入者数 約 1692 万契約

ADSL (1255 万) FTTH (160 万) CATV (277 万)

携帯電話によるインターネットサービス加入者数 約 7193 万契約

(2000 年における日本の総世帯数: 約 4600 万世帯)

ネットワーク接続形態

ここでは、一般的な一戸建用のネットワーク、および集合住宅用のネットワーク接続形態について記述します。

一戸建用のネットワーク

一戸建のネットワークの特徴はコスト高ですが、個人判断で敷設可能で、宅外から回線を直接引き込めるということにあります。

集合住宅用のネットワーク

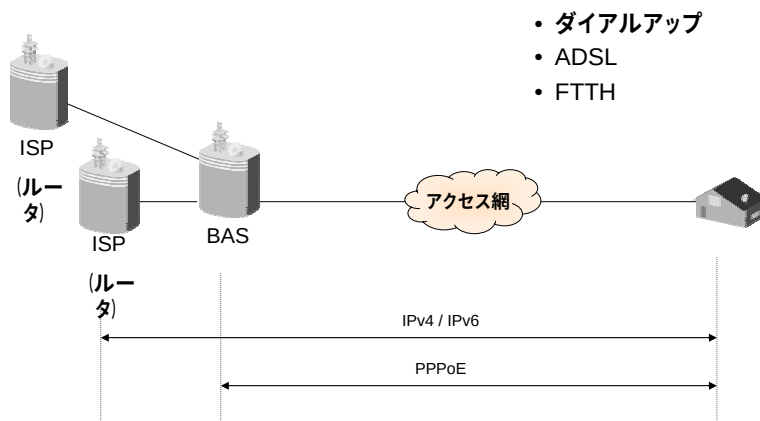
集合住宅用のネットワークは、コストが低いものの、住民の合意が必要 (新規敷設の場合) で、マンションの設備としてなど、インフラ施設として提供されることにあります。

一戸建のネットワークは、下図のように、PPP 接続型と IP 接続型の 2 通りに分けられます。PPP 接続型では、PPPoE セッションをはり、その上で IPv4 あるいは IPv6 を通すことになります。一方、IP 接続型では、アクセス網が ISP 側のルータと直結するシンプルな構成となっています。

1.4.2. 現状の分析 (ネットワーク接続形態)

■ 一戸建住宅用ネットワーク接続形態

ケース1: PPP接続型



Oct 8, 2004

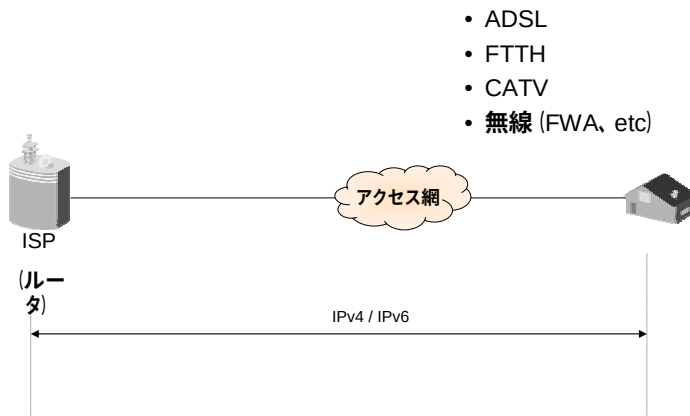
IPv6PC Transition WG Home SWG

45

1.4.2. 現状の分析 (ネットワーク接続形態)

■ 一戸建住宅用ネットワーク接続形態

ケース2: IP接続型



Oct 8, 2004

IPv6PC Transition WG Home SWG

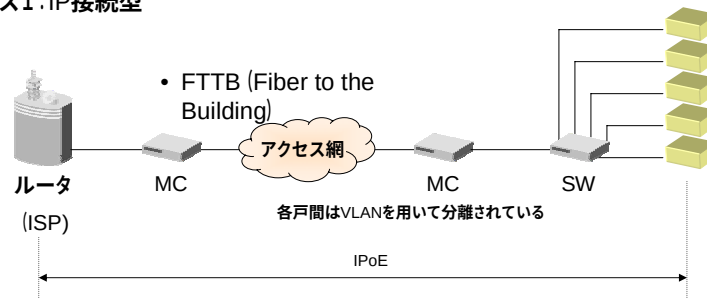
46

集合住宅の場合も IP 接続型と PPP 接続型に分けることができます。双方とも、集合住宅内にはスイッチが置かれ、各世帯は VLAN によって分離されていて直接通信ができないようになっています。さらに、認証サーバ兼ルータを、集合住宅内に設置するケースがあります。

1.4.2. 現状の分析 (ネットワーク接続形態)

■ 集合住宅用ネットワーク形態

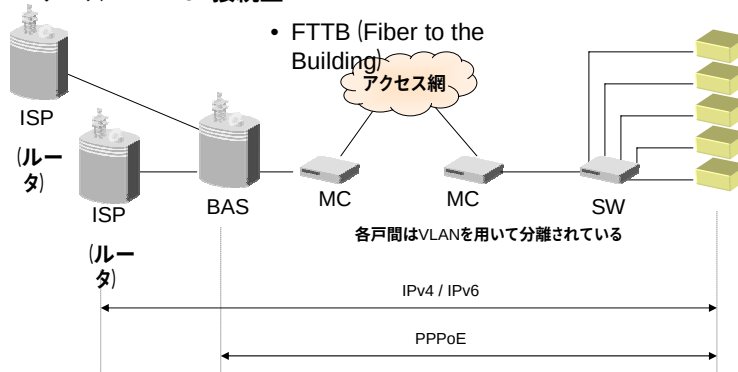
ケース1: IP接続型



1.4.2. 現状の分析 (ネットワーク接続形態)

■ 集合住宅用ネットワーク形態

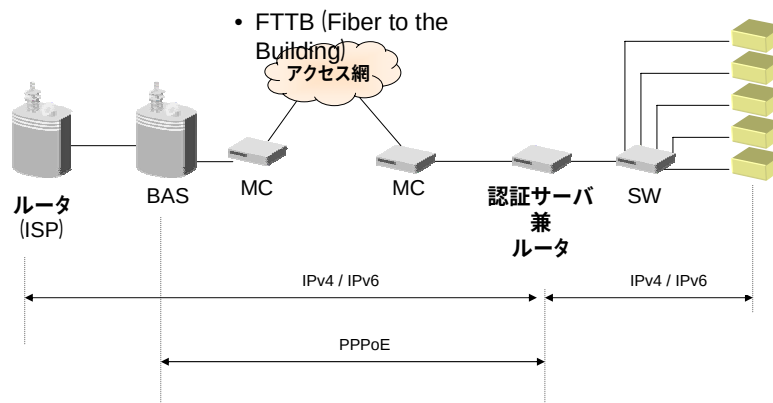
ケース2: PPPoE接続型



1.4.2. 現状の分析 (ネットワーク接続形態)

■ 集合住宅用ネットワーク形態

ケース3: 集合住宅内認証サーバ設置型



Oct 8, 2004

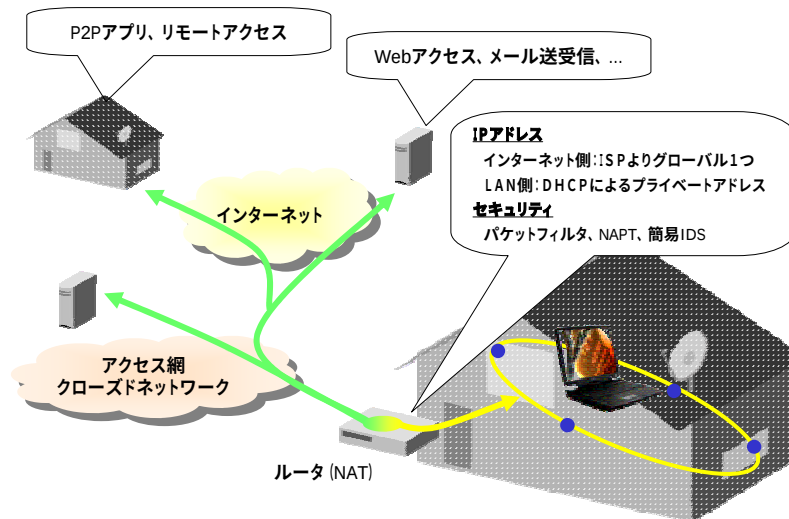
IPv6PC Transition WG Home SWG

49

典型例

現在のIPv4によるホームネットワークは、下図のような形態が典型的です。家庭とインターネットの境界に置かれたルータは、インターネット側インタフェースにISPがグローバルアドレスを1個割り振り、LAN側のインタフェースではルータのDHCPサーバ機能によってプライベートアドレスを割り振って、相互間のアドレス変換(NAT)が行われています。家庭からは、インターネット経由でWebやFTP、メールなどの基本ツールに加え、P2Pアプリケーションやリモートアクセスなどが活用されています。アクセス網では一部、クローズドネットワークに接続されています。

1.4.3. 現状の分析 (IPv4ホームネットワークの典型例)



Oct 8, 2004

IPv6PC Transition WG Home SWG

51

家庭内概略

現在、エンド機器としては、PCのほか、エンターテインメント機器としてゲーム機やAV機器が利用されるようになってきています。PC上のデータをテレビで再生可能とするネットワークプレイヤーが登場し、DLNAのガイドラインへの対応が進むなどにより、相互連携可能な機器、ソフトが登場しつつあります。PCとNon-PC間の接続だけでなく、Non-PC間の連携も可能になりつつあります。

くらし関連機器については、白物家電でネットワーク対応の製品が、一部メーカより試験的に登場しました。しかし、普及はまだ先のことになると考えられます。ネットワーク対応カメラやネットワーク対応センサーも販売されていますが、数は少ないのが現状です。保育所などに設置されたカメラを利用するユーザがいるのは事実です。

クリエイティブ機器も数は少なく、コミュニケーション機器ではIP電話が急速に普及しつつあります。IPテレビ電話への発展も期待されています。

家庭内の配線は有線あるいは無線(802.11a/b/g)によって行われています。

ネットワーク機器は、ホームゲートウェイ、メディアコンバータ、ルータなどのアクセス網終端装置が一般的です。

利用サービスは、Web、メール(クライアントの立場で利用)、メッセージ系(P2P利用)、家庭内のメール・Webサーバ(サーバの立場で利用:ごく一部ユーザのみ)、リモートからのビデオ予約など(一部サービスイン)などです。

セキュリティについては、ルータにおけるファイアウォール機能(パケットフィルタとNAPT機能

が中心、一部ステートフルパケットインスペクション機能や簡易 IDS など)、PC におけるパーソナルファイアウォール機能 (メールのウィルスチェック中心)、ISP 提供サービス (ウィルスチェックなど) が行われています。

しかし、基本はパケットフィルタ/NAT による incoming packet の制限であり、ほとんどのユーザはデフォルト設定以上のことはまずできません。

2.ホームネットワークにおける移行シナリオ

ホームネットワークにおける移行シナリオの考え方

移行モデルとシナリオの考え方

現在の家庭の状態としては、ルータ接続による複数機器接続が行われている場合、モデム（ダイヤルアップ、ADSL モデム、メディアコンバータ）接続による1台のみの接続（ブリッジ接続）の場合、そしてネットワークと対応機器のどちらもない場合があります。

ここでは、基本として PC、Non-PC 混在状況での IPv6 移行のシナリオを考えます。SOHO セグメントとの共通課題も数多く存在しますが、ホームならではの Non-PC のみの環境におけるシナリオの考慮が必要となります。

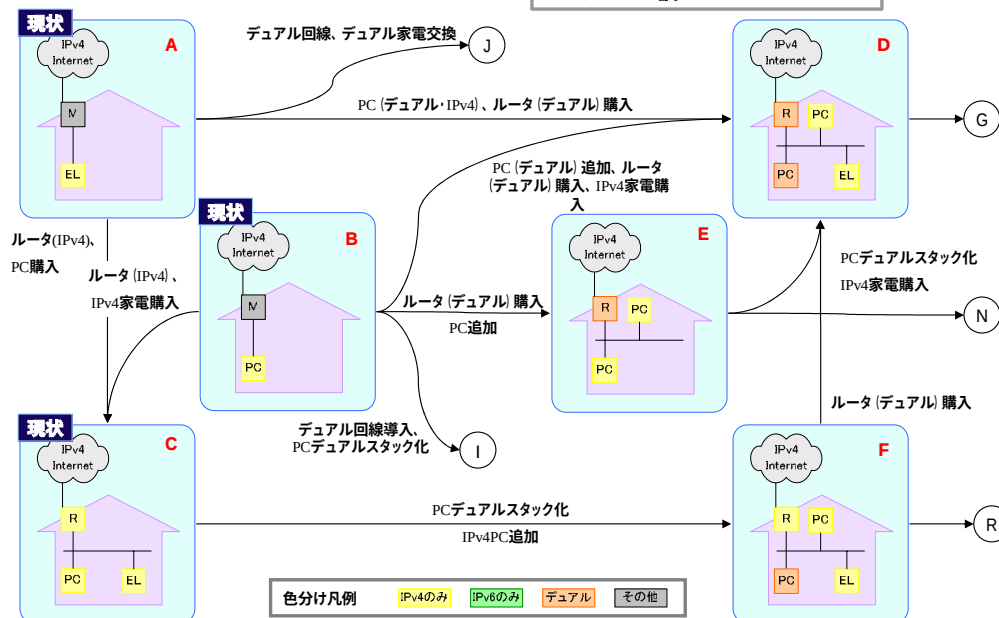
以下では、現状、BCP、IPv6 普及期のそれぞれの状態における家庭のモデルを想定し、そのモデル間の差分を明確にすることで、移行における課題を整理します。

ホームネットワークにおける移行シナリオ（移行モデル概要）

ホームネットワークの現状から BCP、IPv6 普及期に至る移行プロセスは、下の 3 つの図のよう
に要約することができます。

2.2. 概要 (現状からBCPへ)

<凡例>
R: ルータ M: モデム、メディアコンバータ
B|R: IPv6ブリッジ搭載IPv4ルータ
EL: 家電機器 PC: パソコン
TE: リモートの端末

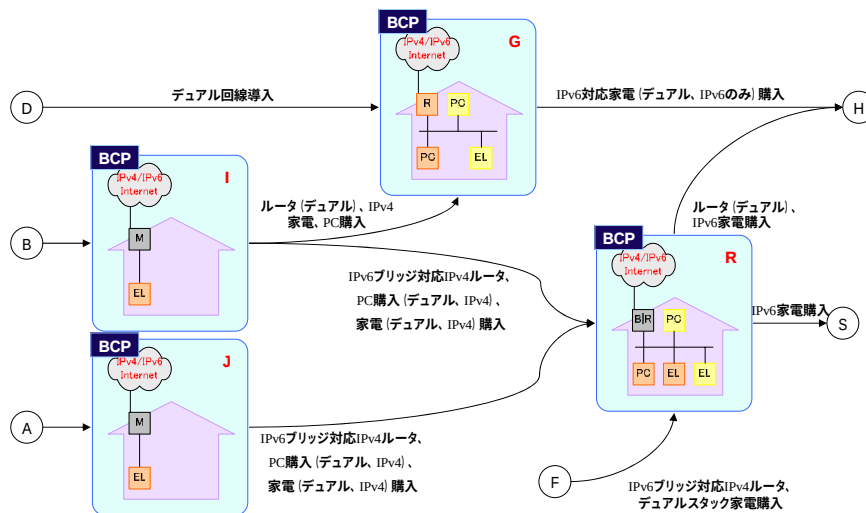


Oct 8, 2004

IPv6PC Transition WG Home SWG

59

2.2. 概要 (BCP)

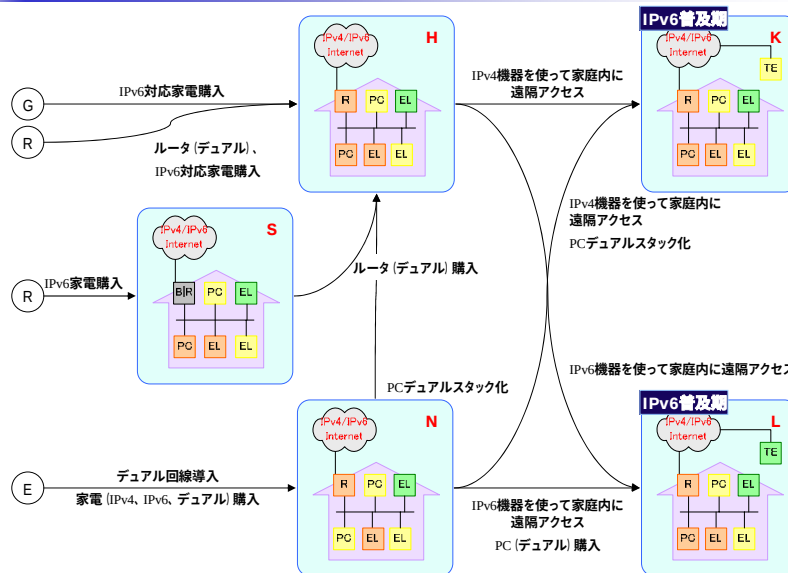


Oct 8, 2004

IPv6PC Transition WG Home SWG

60

2.2. 概要 (BCPからIPv6普及期へ)



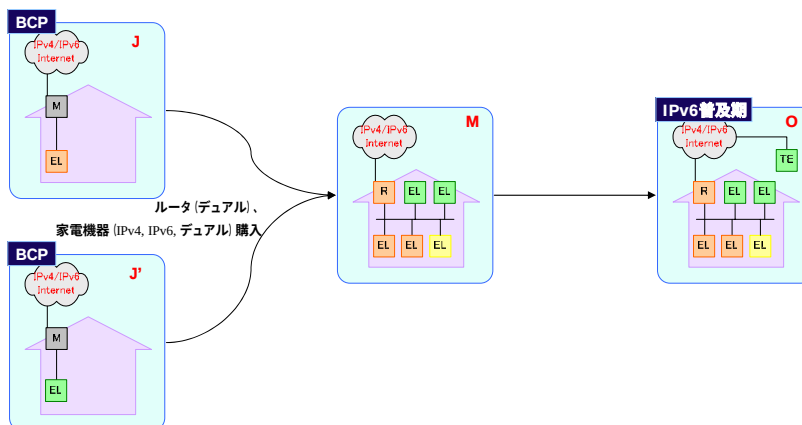
Oct 8, 2004

IPv6PC Transition WG Home SWG

61

PC の利用がまったくなく、Non-PC の利用に伴って IPv6 への移行が進むシナリオについては、下の図のように想定することができます。

2.2. 概要 (non-PCモデルの場合)



Oct 8, 2004

IPv6PC Transition WG Home SWG

62

ホームネットワークにおける移行シナリオ（シナリオ検討）

上の図では、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) からモデル G (BCP) 経由でモデル K・L (IPv6 普及期) へ向かうのがもっとも展開的なシナリオと考えられます。また、実際にサービスされている例としては、A、B、C から R を経由して K、L へと到達する移行シナリオもあります。

家庭セグメントで考慮が必要な他のシナリオとしては、まず、PC を持たないような家庭が、家電やゲーム機のみを持つことにより、J、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。

各想定モデルについては、以下の項目で定義します。

- ・構成 (アクセス網、インターネットとの接続点、ホームネットワーク内の機器)
- ・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 (ISP から割り当てられるアドレスと、家庭内に割り当てるアドレス)
- ・ネーミング (クエリや登録の方法)
- ・セキュリティ対策 (暗号化、不正アクセス対応、ウイルス対策、DoS 対策)
- ・設定方法 (機器の設定方法)

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: モデム／メディアコンバータ＋Non PC (ゲーム機、HDD レコーダなど)

PC もない状態で、ゲーム機などの Non-PC 機器を 1 台だけ接続している場合です。

B: モデム／メディアコンバータ＋PC

PC を 1 台だけ接続している場合です。

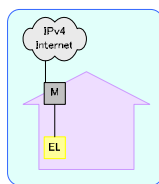
C: ルーター＋家庭内 LAN を構築

これはルーターを配置するとともに家庭内 LAN を構築、複数台の機器によるインターネット接続を実現している場合です。

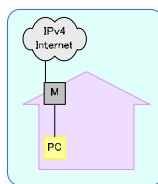
2.3.2. モデルの想定:現状

■ 現状 (IPv4) でのホームネットワークの例

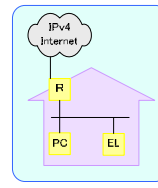
- A モデム/MC+non-PC (ゲーム機、HDDレコーダなど)
- B モデム/MC+PC
- C ルーター+家庭内LANを構築



モデルA



モデルB



モデルC

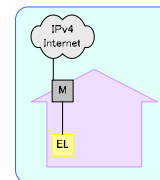
モデル A の特徴は、下の図の通りです。モデムやコンバーターによるブリッジ接続で、1 台の Non-PC 端末のみが接続されています。PPP、DHCP によってこの端末にはグローバル IP アドレスが与えられていて、外部から家庭内の機器へのアクセスが必要な場合は、ダイナミック DNS サービスが利用されます。

2.3.2. モデルの想定：現状 (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	モデムやメディアコンバータ (ブリッジ接続)
	接続機器	ゲーム機・non-PC機器 (AV機器・IPカメラ・IP電話など) 複数機器を切り替えてつなぐ場合を含む
利用アプリ	ネットワークゲーム、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に指定されたDNSサーバ (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 (登録手法は利用サービスに依存)
設定方法	なし	
その他		

モデルA



Oct 8, 2004

IPv6PC Transition WG Home SWG

67

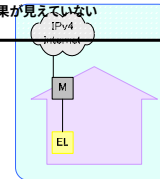
セキュリティ対策に関しては、モデル A の場合、通信の暗号化、不正アクセス対応ともに、機器によって異なり、対策が実施されていないケースも多くあります。ウイルス対策については、対応されていません。

2.3.2. モデルの想定：現状 (モデルAの特徴)



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	機器に依存 - IPsec - SSL - 独自 などの方式を実施、または実施していない	- HTTPなどTCPベースであればSSLが一般的 - IPsec対応機器も数点ある	- 通信内容が盗聴される可能性がある - 通信内容が改竄される可能性がある - UIの煩雑化 - IPsec利用時の鍵設定
	不正アクセス対応	機器に依存 - ユーザ認証 - サーバ認証 - クライアント認証 - アドレスベースのアクセス制限 または実施していない	- 機器が提供するサービスを不正に利用されないための適切な認証を実施する - IPアドレスベースのアクセス制限を実施する	- サービスを不正に利用される可能性がある - カメラ等の場合、プライバシーの漏洩につながる - 対策未実施の機器、サービスの場合、脅威に当たる確率が低いので問題視されていない
	ウイルス対策	対策していない	—	- ウイルスに対する脅威が存在しないと考えられている - 対策に対する効果が見えていない

モデルA



Oct 8, 2004

IPv6PC Transition WG Home SWG

68

次にモデル B の特徴は、下の図の通りです。モデムやコンバータによるブリッジ接続で、1 台

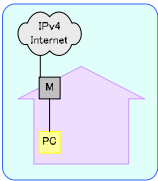
の PC 端末のみが接続されています。PPP、DHCP によってこの端末にはグローバル IP アドレスが与えられていて、外部から家庭内の機器へのアクセスが必要な場合は、ダイナミック DNS サービスが利用されます。

2.3.2. モデルの想定：現状 (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	モデムやメディアコンバータ (ブリッジ接続) 複数機器を切り替えてつなぐ場合を含む
	接続機器	PC
利用アプリ	Mail、WEB、ネットワークゲーム、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に指定されたDNSサーバ (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 (登録手法は利用サービスに依存)
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B

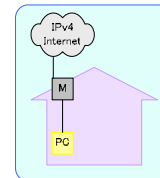


モデル B におけるセキュリティ対策は、通信の暗号化に関しては OS やアプリケーションに依存し、不正アクセスやウイルスへの対策は、ユーザに任されているのが現状です。

2.3.2. モデルの想定：現状 (モデルBの特徴)

セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	OS・アプリに依存 - IPsec - SSL - 独自 などの方式 または実施していない	- 個別に対応 - 粒度は様々 - アプリ単位 - プロトコル単位 - アドレス単位 - TCPベースであればSSLが一般的 - 接続相手に応じて柔軟に対応を要可能	- 通信内容が盗聴される可能性がある - 通信内容が改竄される可能性がある - IPsecは一般家庭では使いにくい - ただし、会社のイントラアクセス用に専用アプリケーションとして提供されている例は多い - ユーザは種々のダイアログボックスを確認せずに「OK」ボタンを押してしまっている
	不正アクセス対応	ユーザに依存	パーソナルファイアウォール	- PC上のセキュリティホールを攻撃される可能性がある - 動かないアプリがあると一括してパーソナルファイアウォールを停止するユーザも多い
	ウイルス対策	ユーザに依存	・ウイルスチェッカー ・ISPのサービス	- ウイルスに感染する／感染を広める - ウイルスによって情報が外部に流出する - パフォーマンスを理由にウイルスチェッカーをはずしてしまうユーザがいる

モデルB



Oct 8, 2004

IPv6PC Transition WG Home SWG

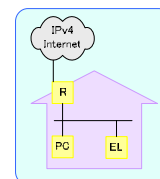
70

モデルCは、ルータを使ったいわゆるブロードバンド接続環境の家庭です。現状ではIPv4のみのネットワークサービスがほとんどですが、ルータで家庭内のLANと接続され、この家庭内LANにはPCやNon-PC機器が複数台接続されています。LAN側ではDHCPによってプライベートアドレスが配布されています。戸外から家庭内のLANにつながれた機器へのアクセスには、ダイナミックDNSサービスなどが利用されています。

2.3.2. モデルの想定：現状 (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・non-PC機器 (AV・家電機器、IPカメラ、IP電話)
利用アプリ	Mail、WEB、ネットワークゲーム、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	DHCP
ネーミング	クエリ	(内→外) ISPに指定されたDNSサーバを利用、宅内ノード向けにルータで中継 (外→内) DDNSサービスやベンダー提供の専用サーバの利用 (ただし、ルータを越えるアクセスを実現するには設定が必要) (内→内) NetBIOSなど
	登録	外部向け：DDNSやベンダー提供の専用サーバの利用 (登録手法は利用サービスに依存)
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



Oct 8, 2004

IPv6PC Transition WG Home SWG

71

モデルCのセキュリティ対策は、通信の暗号化に関しては、機器、OS、アプリケーションに依存

します。不正アクセスに関しては、ルータでは対応していますが、これをどのように利用するかに関してはユーザに依存します。エンド端末レベルのセキュリティは、機器やユーザに依存します。ウイルス対策は、ルータにおける対応はなく、エンド端末ではユーザに依存します。

2.3.2. モデルの想定：現状 (モデルCの特徴)



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	- 機器、OS、アプリに依存 - IPsec - SSL - 独自などの方式または実施していない	- ルータ： - PPTP, IPsecの終端 - パススルー - エンドノード： - 機器・アプリで個別に暗号化を行う - 接続相手に応じて対応が変化 - ルータがエンドノードの肩代わりできる場合はそれを使用するケースもある	モデルA、Bと同じ エンドノードの通信をルータが守る場合には、手動設定が必要(エンドノードが守ってほしい通信をルータに教える手段が無いため)
	不正アクセス対応	- ルータ - 対策済み - ただし実施はユーザに依存 - エンドノード - 機器、ユーザに依存	- ルータ - パケットフィルタ - 簡易IDS - エンドノード - パーソナルファイアウォール	モデルA、Bと同じ
	ウイルス対策	- ルータ - 対策していない - エンドノード - ユーザに依存	- ルータ - ウイルスチェッカー(通過するパケットに対して) - エンドノード - ウイルスチェッカー - ISPのサービスを利用する	モデルA、Bと同じ - 家電機器に対する脅威の洗い出しが完了していない - NASなどからウイルスが広まる可能性 - 外部ストレージを家電機器に接続した際にストレージ内にウイルスが混入する可能性 - 家電機器がウイルスに侵入されても気づかない可能性がある - ルータに対するウイルスの脅威は存在しない(と考えられている)

Oct 8, 2004

IPv6PC Transition WG Home SWG

72

モデルの想定：最初の一步

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するが、あくまでもIPv4で利用し、買ったならIPv6も付いてきた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。

この一歩進んだ形態のモデルが、モデルD、モデルE、モデルFです。それぞれは次のようなケースを意味しています。

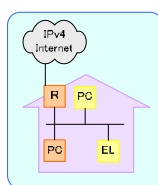
モデルD：ルータもPCもデュアルスタック対応だった

モデルE：ルータを買ったらデュアルスタック対応だった

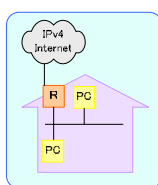
モデルF：PCを買ったらOSがデュアルスタック対応だった(Windows XPなど)

2.3.3. モデルの想定：最初の一步

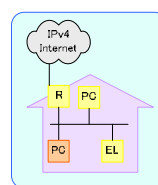
- 現状から一步進むとすると・・・
 - IPv6も利用可能な機器は登場している
 - IP電話
 - ネットワークカメラ など
 - 複数機器を利用する際にはルータの利用を推奨
- モデル
 - D: ルータもPCもデュアルスタック対応だった
 - E: ルータを買ったらデュアルスタック対応だった
 - F: PCを買ったらOSがデュアルスタック対応だった



モデルD



モデルE



モデルF

モデルD、E、Fの特徴は基本的に同じなので、ここではモデルDについてのみ説明し、E、Fについては省略します。このモデルでは、家庭内にPC、あるいはこれに加えてNon-PCが複数台存在し、ルータで外部と接続されています。ルータのインターネット側インタフェースにはDHCP、PPPでグローバルIPアドレスが割り当てられ、家庭内ではDHCPによってプライベートアドレスが割り当てられます。

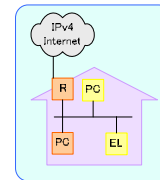
2.3.3. モデルの想定：最初の一步 (モデルDの特徴)



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・non-PC機器 (AV・家電機器、IPカメラ、IP電話)
利用アプリ	Mail、WEB、ネットワークゲーム、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
	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
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D



Oct 8, 2004

IPv6PC Transition WG Home SWG

74

モデルDのセキュリティ対策は、通信の暗号化に関しては、機器、OS、アプリケーションに依存します。不正アクセスに関しては、ルータでは対応していますが、これをどのように利用するかに関してはユーザに依存します。エンド端末レベルのセキュリティは、機器やユーザに依存します。ウイルス対策は、ルータにおける対応はなく、エンド端末ではユーザに依存します。

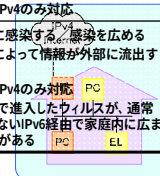
2.3.3. モデルの想定：最初の一步 (モデルDの特徴)



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

セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	機器、OS、アプリに依存 ■ IPsec ■ SSL ■ 独自 などの方式 または実施していない	■ ルータ ■ PPTP、IPsecの終端 ■ パススルー ■ エンドノード ■ 機器・アプリで個別に暗号化 ■ 接続相手に応じて対応が変化 ■ ルータがエンドノードの肩代わりをできる場合はそれを使用するケースがある	◆ 通信内容が盗聴される可能性がある ◆ 通信内容が改竄される可能性がある ■ いずれもIPv4のみ対応 ■ IPv6の外部接続は無いので利用場がない
	不正アクセス対応	■ ルータ ■ 対策済み ■ ただし実施はユーザに依存 ■ エンドノード ■ ユーザ、機器に依存	■ ルータ ■ パケットフィルタ ■ 簡易IDS ■ エンドノード ■ パーソナルファイアウォール	◆ サービスを不正に利用される可能性がある ◆ カメラ等の場合、プライバシーの漏洩につながる ◆ PC上のセキュリティホールを攻撃される可能性がある ■ いずれもIPv4のみ対応
	ウイルス対策	■ ルータ ■ 対策していない ■ エンドノード ■ 機器、ユーザに依存 ■ ISPのサービスを利用する	■ ルータ ■ ウィルスチェッカー (通過するパケットに対して) ■ エンドノード ■ ウィルスチェッカー ■ ISPのサービス	◆ ウィルスに感染する ◆ 感染を拡大する ◆ ウィルスによって情報が外部に流出する ■ いずれもIPv4のみ対応 ■ IPv4経由で進入したウィルスが、通常は利用しないIPv6経由で家庭内に広まる可能性がある

モデルD



Oct 8, 2004

IPv6PC Transition WG Home SWG

75

モデルの想定：BCP

次に IPv6 における BCP 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。この時点で、家庭は 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 サービスへ変更します。IPv4 も従来どおり利用可能です。

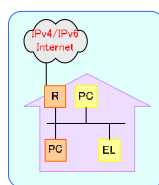
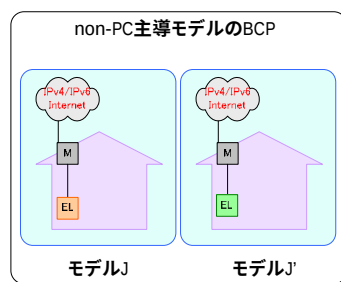
IPv6 ルータが利用できない場合、IPv4 ルータの IPv6 ブリッジ機能を利用する選択肢も考えられます。これが下図のモデル R です。

一方で、Non-PC 機器主導のシナリオも考えられます。一部では、たとえば IP 電話やセットトップボックス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 対応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、J' から始まることになります。

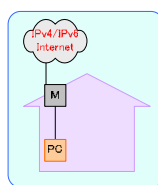
2.3.4. モデルの想定：BCP



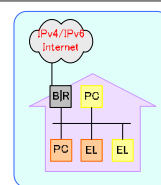
- 一部IPv6化：IPv6普及へのBCPモデル
 - 一部機器だけでもIPv6としてサービスを利用開始
 - プロバイダのIPv6サービスに新規加入・変更
 - IPv4も従来どおり利用可能
 - IPv6ルータが利用できない場合、IPv6ブリッジ機能を利用する方法もある(モデルR)
- いきなりモデルJ、J'から始まる場合もある
 - non-PC主導シナリオ
 - サービス一体型のIPv6家電 (IP電話、STB) など



モデルG



モデルI



モデルR

モデル G では、家庭内 LAN 上の PC のみが IPv6 を利用し、他は IPv4 のみを使っています。

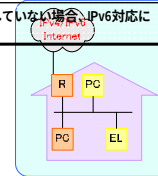
2.3.4. モデルの想定:BCP (モデルGの特徴)



(IPv4部分についてはモデルC/Dと同じなので省略する)

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はデュアルスタック	
構成	ネットワークとの境界	ルータ (デュアルスタック) 接続
	接続機器	PC・ゲーム機・non-PC機器 (AV、家電機器、IPカメラ、IP電話)
利用アプリ	従来と同様 (WEB、会社のイントラと接続、など)、IP電話、IP放送など	
アドレス	インターネット側	リンクローカルのみ
	ローカル側	LAN側で使うプレフィックス ■ DHCPv6-PD、DTCPPなどによりISPから取得 (/48、/64が割り当てられる) ■ 自動トンネルプロトコルによる生成 ■ 静的割り当て RAでプレフィックスを通知、リンクローカル
ネーミング	クエリ	Windows XPのIPv6ではIPv6を使ったDNSパケットの転送は出来ない
	登録	Windows XP SP1までのスタックにはAAAAとCNAMEの処理に問題があり、通信できない場合がある
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	OSがIPv6に対応していても、アプリケーションがIPv6に対応していない場合、IPv6対応に制限がある場合がある。	

モデルG



Oct 8,2004

IPv6PC Transition WG Home SWG

77

モデル G の IPv6 に関するセキュリティ対策は、通信の暗号化に関しては、機器、OS、アプリケーションに依存します。不正アクセスに関しては、ルータでは対応していますが、これをどのように利用するかに関してはユーザに依存します。エンド端末レベルのセキュリティは、機器やユーザに依存します。ウイルスについては、IPv6 では現状、対応策がありません。

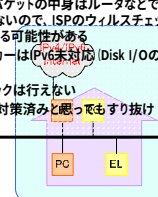
2.3.4. モデルの想定:BCP (モデルGの特徴)



(IPv4部分についてはモデルC/Dと同じ)

セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	機器、OS、アプリに依存 ■ IPsec ■ SSL ■ 独自などの方式 - または実施していない	■ ルータ ■ IPsecの終端 ■ エンドノード ■ 機器・アプリで個別に暗号化 ■ ルータがエンドノードの肩代わりをできる場合はそれを使用するケースがある (IPsec Tunnelモードなど)	■ Windows XPはIPv6 ESPで暗号化できない (2004/10/01現在) ■ エンドノードが暗号化をルータに依頼する仕組みが必要 (または手設定が必要) ■ エンドノードがIPsecを利用する際にはUIが複雑化する (要求スキルが急激に上がる)
	不正アクセス対応	■ ルータ ■ 対策済み ■ 実施はユーザに依存 ■ エンドノード ■ ユーザ、機器に依存	■ ルータ ■ パケットフィルタ ■ エンドノード ■ パーソナルファイアウォール	◆ IPv6接続を利用した時点で始めてエンドノードがインターネットからダイレクトにアクセスされる可能性がある (未対策セキュリティホールの顕在化) ◆ デュアルスタックホストを介した家庭内IPv4ノードへの不正アクセスの可能性 ■ IPv6対応のパーソナルファイアウォール製品が存在しない (Windows XP SP2標準品のみ)
	ウイルス対策	IPv6は対策なし	—	◆ 暗号化されたパケットの中身はルータなどではチェックできないので、ISPのウイルスチェックなどを通過する可能性がある ■ ウイルスチェッカーは (IPv6未対応) (Disk I/Oのみチェック) ■ 通信チェックは行えない ■ ユーザが対策済みと誤って取り除ける可能性

モデルG



Oct 8,2004

IPv6PC Transition WG Home SWG

78

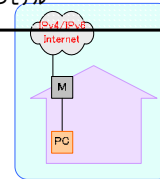
モデルⅠは、モデルⅡのPCが1台しかない環境で、このPCがデュアルスタック対応のものに置き換わったという状態です。利用したいアプリケーションがIPv6にしか対応していない場合はこのモデルに意味がありますが、そうでない場合はIPv4接続しか使われません。

2.3.4. モデルの想定:BCP (モデルⅠの特徴)



モデル	Ⅰ:Ⅱ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が1台、PCはデュアルスタック	
構成	ネットワークとの境界	モデム、メディアコンバータ(ブリッジ接続)
	接続機器	PC
利用アプリ	インターネット、クローズドネットワーク(地域IP網)と接続 WEB、会社のイントラと接続、IP放送など	
アドレス	インターネット側	次のいずれかの方法でグローバルプレフィックスを取得 ■ DHCPv6-PD、DTCPPなどによりISPから取得(/48、/64が割り当てられる) ■ 自動トンネルプロトコルによる生成 ■ 静的割り当て ■ ISPから直接RAを受ける
	ローカル側	— (1台のためローカルという概念が存在しない)
ネーミング	クエリ	ISPに指定されたDNSサーバ、外部からはDDNS利用
	登録	外部向け:DDNSやベンダー提供のサーバを利用する(登録手法は利用サービスに依存)
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IPv6のみに対応している場合に意味を持つモデル そうでない場合はIPv4接続しか使用されない	

モデルⅠ



Oct 8,2004

IPv6PC Transition WG Home SWG

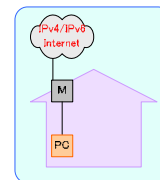
79

モデルⅠの IPv6 に関するセキュリティ対策は、通信の暗号化に関しては、機器、OS、アプリケーションに依存します。不正アクセスに関しては、ユーザに依存します。ウイルスについては、IPv6 では現状、対応策がありません。

2.3.4. モデルの想定:BCP (モデルIの特徴)



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	OS、アプリに依存 ■ IPsec ■ SSL ■ 独自 などの方式 または実施していない	OSやアプリで個別に暗号化	■ Windows XPはIPv6 ESPで暗号化できない(2004/10/01現在) ■ エンドノードがIPsecを利用する際にはUが複雑化する(要求スキルが急激に上がる)
	不正アクセス対応	ユーザに依存	■ パーソナルファイアウォール ■ Windows XP SP2対応済	■ IPv6対応の市販パーソナルファイアウォールソフトが無い ■ Windows XP装備品はパケットフィルタ機能のみ
	ウィルス対策	IPv6は対策なし	-	■ ウィルスチェッカーはIPv6未対応(Disk I/Oのみチェック) ■ 通信チェックは行えない ■ ユーザが対策済みと思ってもすり抜ける可能性



モデルI

Oct 8,2004

IPv6PC Transition WG Home SWG

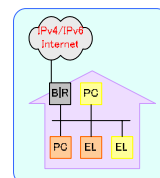
80

モデル R は、モデル B において PC がデュアルスタック対応のものに置き換わった状態です。IPv6 対応のルータは導入されていませんが、IPv4 ルータの IPv6 ブリッジ機能で IPv6 を家庭内 LAN に通しています。

2.3.4. モデルの想定:BCP (モデルRの特徴)



モデル	R : IPv6ルータを利用せずにIPv6に対応したPCや機器が導入された	
説明	宅内にPCが1台以上、PCと機器はデュアルスタックまたはIPv4のみ	
構成	ネットワークとの境界	IPv4ルータ、IPv6ブリッジ
	接続機器	PC・ゲーム機・non-PC機器(AV、家電機器、IPカメラ、IP電話)
利用アプリ	インターネット、クローズドネットワーク(地域IP網)と接続 WEB、会社のイントラと接続、IP放送など	
アドレス	インターネット側	IPv6ブリッジを通過したRAでそのままアドレスをつける (IPv6ブリッジなので、WAN/LANの区別なし)
	ローカル側	—
ネーミング	クエリ	ISPに指定されたDNSサーバ、外部からはDDNS利用
	登録	外部向け: DDNSやベンダー提供のサーバを利用する
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IPv6のみに対応している場合に意味を持つモデル そうでない場合はIPv4接続しか使用されない	



モデルR

Oct 8,2004

IPv6PC Transition WG Home SWG

81

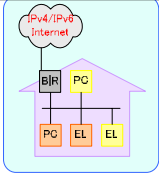
モデル R の IPv6 セキュリティ対策ですが、暗号化通信に関しては PC の OS やアプリケーション

ンに依存します。不正アクセスに関しては、IPv6 ブリッジを使う限り対策はありません。RA プロキシ対応製品なら不正アクセスの防止に役立ちますが、利用するかどうかはユーザに依存します。

2.3.4. モデルの想定：BCP (モデルRの特徴)



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	OS、アプリに依存 ■ IPsec ■ SSL ■ 独自 などの方式 または実施していない	OSやアプリで個別に暗号化	■ Windows XPはIPv6 ESPで暗号化できない(2004/10/01現在) ■ エンドノードがIPsecを利用する際にはUが複雑化する(要求スキルが急激に上がる)
	不正アクセス対応	■ IPv6ブリッジは対策なし ■ RA Proxy対応製品は対策済み ■ ユーザに依存	エンドノード ■ パーソナルファイアウォール ■ Windows XP SP2対応済 ■ 市販パーソナルファイアウォール製品のv6化まだ ■ IPv6ブリッジ ■ パケットフィルタリング	■ IPv6ブリッジは全IPv6パケットを転送してしまうので、IPv4と同等のセキュリティを保つことが難しい ■ IPv6対応の市販パーソナルファイアウォールソフトが無い ■ Windows XP装備品はパケットフィルタ機能のみ
	ウィルス対策	IPv6は対策なし	-	■ ウィルスチェッカーはIPv6未対応(Disk I/Oのみチェック) ■ 通信チェックは行えない ■ ユーザが対策済みと思ってもすり抜ける可能性



モデルR

Oct 8,2004

IPv6PC Transition WG Home SWG

82

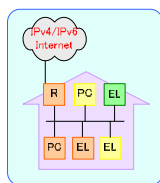
モデルの想定：IPv6 普及期夜明け前

BCP の状態から、IPv6 普及期に向けて 1 歩踏み出したのがモデル H、N、S です。この状態では、IPv6 のみに対応した機器が現れています。しかし、エンドユーザには IPv6 と IPv4 の違いが分からないため、IPv4 機器との通信が必要なものについては IPv4 と IPv6 間のプロトコルトランスレータ機能が求められます。

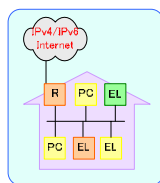
2.3.5. モデルの想定：IPv6普及期夜明け前



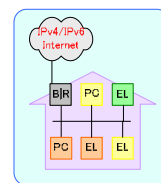
- BCPよりさらに1歩進んでみる
 - IPv6のみ対応する機器が登場
 - ユーザの観点からは、IPv6のみの機器とIPv4のみの機器の違いは不明
 - 機器が汎用であればあるほど、IPv4機器とも通信できるようにしたい、という要求が強くなる
 - トランスレータ機能が必要
 - モデルNの場合にはPCはIPv4のみ、家電がIPv6／デュアル



モデルH



モデルN



モデルS

Oct 8, 2004

IPv6PC Transition WG Home SWG

83

モデル H は、モデル G において、IPv6 のみに対応した機器が導入されたケースです。デュアルスタック対応のルータで ISP と接続されています。

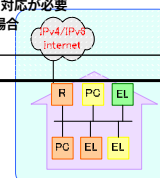
2.3.5. モデルの想定：IPv6普及期夜明け前 (モデルHの特徴)



(IPv4部分についてはモデルC/Dと同じ)

モデル	H : モデルG + IPv6のみ対応の機器を購入	
説明	宅内にPC/機器が複数台、一部PCはデュアルスタック、一部はIPv6のみ対応	
構成	ネットワークとの境界	ルータ(デュアルスタック)接続
	接続機器	PC・ゲーム機・non-PC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IPv6機器同士の通信、IP放送	
アドレス	インターネット側	次のいずれかの方法でグローバルプレフィックスを取得 ■ DHCPv6-PD、DTCPPなどによりISPから取得 (/48、/64が割り当てられる) ■ 自動トンネルプロトコルによる生成 ■ 静的割り当て ■ ISPから直接RAを受ける
	ローカル側	RAプレフィックスを通知する リンクローカル
ネーミング	クエリ	(外→内) 個々のノードがDDNSサーバに登録
	登録	(内→内) UPnPのIPv6対応版 (未定)、マルチキャストDNS、など
設定方法	トランスレータの設定に関しては、トランスレータの方式ごとに対応が必要 ■ 変換用に専用プレフィックスを用意しなければならない場合 ■ IPv4アドレスとの事前対応づけが必要な場合	
その他	トランスレータの位置は検討必要	

モデルH



Oct 8, 2004

IPv6PC Transition WG Home SWG

84

モデル H での IPv6 セキュリティに関しては、不正アクセスやウイルスへの対策として、端末用

のセキュリティ製品が IPv6 対応することが望めます。

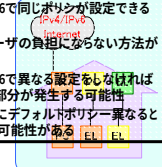
2.3.5. モデルの想定: IPv6普及期夜明け前 (モデルHの特徴)



(IPv4部分についてはモデルC/Dと同じ)

セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	実装度合い、方式ともにOS、機器・アプリに依存する ■ IPsec ■ SSL ■ 独自 などの方式 または実施していない	■ ルータ ■ IPsecの終端 (トンネル、トランスポートモード) ■ IPsecなどのパススルー ■ エンドノード ■ IPsec, SSL, 独自方式を機器・アプリで個別に対応 ■ ルータがエンドノードの肩代わりをできる場合はそれを使用するケースがある	■ トランスレータとIPsecの両立
	不正アクセス対応	■ ルータ対策済み ■ エンドノードはユーザに依存 ■ パーソナルファイアウォールがIPv6対応することが望まれる	■ ルータ ■ パケットフィルタ ■ エンドノード ■ パーソナルファイアウォール	◆ 家電機器とPCなどのセキュリティポリシーの不一致による脆弱性の発現 ◆ デュアルスタックホストを介した家庭内IPv4ノードへの不正アクセスの可能性 ◆ トランスレータを利用した予期しないアクセス経路の確立
	ウィルス対策	■ ウィルスチェッカーがIPv6対応することが望まれる ■ ISPによるウィルスチェックがIPv6対応することが望まれる	■ ルータ ■ ウィルスチェッカー (通過するパケットに対して) ■ エンドノード ■ ウィルスチェッカー ■ ISPのサービス	■ IPv4とIPv6で同じポリシーが設定できるか ■ エンドユーザの負担にならない方法があるか ■ IPv4とIPv6で異なる設定をしなければならぬ部分が発生する可能性 ■ 機器ごとにデフォルトポリシー異なると混乱する可能性がある

モデルH



Oct 8, 2004

IPv6PC Transition WG Home SWG

85

モデル N は、モデル C から派生したもので、宅内の PC は IPv4 のみですが、機器はデュアルスタックで、一部は IPv6 のみに対応しています。

2.3.5. モデルの想定: IPv6普及期夜明け前 (モデルNの特徴)

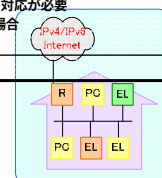


(IPv4部分についてはモデルCと同じ)

モデル	N : モデルC+デュアル／IPv6のみ対応の機器を購入	
説明	宅内にPC/機器が複数台、PCはIPv4のみ、機器はデュアルスタック、一部はIPv6のみ対応	
構成	ネットワークとの境界	ルータ(デュアルスタック)接続
	接続機器	PC・ゲーム機・non-PC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IPv6機器同士の通信、IP放送	
アドレス	インターネット側	次のいずれかの方法でグローバルプレフィックスを取得 ■ DHCPv6-PD、DTCFなどによりISPから取得 (/48、/64が割り当てられる) ■ 自動トンネルプロトコルによる生成 ■ 静的割り当て ■ ISPから直接RAを受ける
	ローカル側	RAプレフィックスを通知する リンクローカル
ネーミング	クエリ	(外→内) 個々のノードがDDNSサーバに登録
	登録	(内→内) UPnPのIPv6対応版 (未定)、マルチキャストDNS、など
設定方法	トランスレータの設定に関しては、トランスレータの方式ごとに対応が必要 ■ 変換用に専用プレフィックスを用意しなければならない場合 ■ IPv4アドレスとの事前対応づけが必要な場合	
その他	トランスレータの位置は検討必要	



モデルN



Oct 8, 2004

IPv6PC Transition WG Home SWG

86

IPv6 セキュリティに関しては、モデル H と同様、エンド端末用のセキュリティ製品が IPv6 対応

する必要があります。

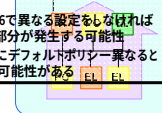
2.3.5. モデルの想定：IPv6普及期夜明け前（モデルNの特徴）



（IPv4部分についてはモデルCと同じ）

セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	実装度合い、方式ともにOS、機器・アプリに依存する ■ IPsec ■ SSL ■ 独自などの方式または実施していない	■ ルータ ■ IPsecの終端（トンネル、トランスポートモード） ■ IPsecなどのパススルー ■ エンドノード ■ IPsec, SSL, 独自方式を機器・アプリで個別に対応 ■ ルータがエンドノードの肩代わりをできる場合はそれを使用するケースがある	■ トランスレータとIPsecの両立
	不正アクセス対応	■ ルータ対策済み ■ エンドノードはユーザに依存 ■ パーソナルファイアウォールがIPv6対応することが望まれる	■ ルータ ■ パケットフィルタ ■ エンドノード ■ パーソナルファイアウォール	■ 家電機器とPCなどのセキュリティポリシーの不一致による脆弱性の発現 ■ デュアルスタックホストを介した家庭内IPv4ノードへの不正アクセスの可能性 ■ トランスレータを利用した予期しないアクセス経路の確立
	ウイルス対策	■ ウィルスチェッカーがIPv6対応することが望まれる ■ ISPによるウイルスチェックがIPv6対応することが望まれる	■ ルータ ■ ウィルスチェッカー（通過するパケットに対して） ■ エンドノード ■ ウィルスチェッカー ■ ISPのサービス	■ IPv4とIPv6で同じポリシーが設定できるか ■ エンドユーザの負担にならない方法があるか ■ IPv4とIPv6で異なる設定をしなければならぬ部分が発生する可能性 ■ 機器ごとにデフォルトポリシー異なると混乱する可能性がある

モデルN



Oct 8,2004

IPv6PC Transition WG Home SWG

87

モデルSは、モデルRにIPv6のみの対応機器が加わった形態です。インターネットとの接続では、IPv4はルーティングされる一方、IPv6はブリッジされています。

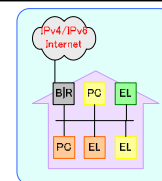
2.3.5. モデルの想定：IPv6普及期夜明け前（モデルSの特徴）



（IPv4部分についてはモデルC/Dと同じ）

モデル	S：モデルR+IPv6のみ対応の機器を購入	
説明	宅内にPC/機器が複数台、一部PCはデュアルスタック、一部はIPv6のみ対応	
構成	ネットワークとの境界	IPv4ルータ、IPv6ブリッジ
	接続機器	PC・ゲーム機・non-PC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IPv6機器同士の通信	
アドレス	インターネット側	IPv6ブリッジを通過したRAでそのままアドレスをつける（IPv6ブリッジなので、WAN/LANの区別なし）
	ローカル側	—
ネーミング	クエリ	（外→内） 個々のノードがDDNSサーバに登録
	登録	（内→内） UPnPのIPv6対応版（未定）、マルチキャストDNS、など
設定方法	トランスレータの設定に関しては、トランスレータの方式ごとに対応が必要 ■ 変換用に専用プレフィックスを用意しなければならない場合 ■ IPv4アドレスとの事前対応づけが必要な場合	
その他	トランスレータの位置は検討必要	

モデルS



Oct 8,2004

IPv6PC Transition WG Home SWG

88

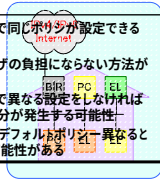
IPv6 セキュリティについては、モデル G と同じことが言えるとともに、トランスレータを利用した際のセキュリティ上のウィークポイントをカバーする必要が出てきます。

2.3.5. モデルの想定：IPv6普及期夜明け前 (モデルSの特徴)



(IPv4部分についてはモデルC/Dと同じ)

セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	実装度合い、方式ともにOS、機器・アプリに依存する - IPsec - SSL - 独自などの方式または実施していない	- ルータ - IPsecの終端 (トンネル、トランスポートモード) - IPsecなどのパススルー - エンドノード - IPsec, SSL, 独自方式を機器・アプリで個別に対応 - ルータがエンドノードの肩代わりをできる場合はそれを使用するケースがある	トランスレータとIPsecの両立
	不正アクセス対応	- IPv6ブリッジは対策なし - RA Proxyの場合は対策済 - エンドノードはユーザに依存 - パーソナルファイアウォールがIPv6対応することが望まれる	- IPv6ブリッジ - パケットフィルタ - エンドノード - パーソナルファイアウォール	- 家電機器とPCなどのセキュリティポリシーの不一致による脆弱性の発現 - デュアルスタックホストを介した家庭内IPv4ノードへの不正アクセスの可能性 - トランスレータを利用した予期しないアクセス経路の確立
	ウイルス対策	- ウイルスチェッカーがIPv6対応することが望まれる - ISPによるウイルスチェックがIPv6対応することが望まれる	- ルータ - ウイルスチェッカー (通過するパケットに対して) - エンドノード - ウイルスチェッカー - ISPのサービス	- IPv4とIPv6で同じポリシーが設定できるか - エンドユーザの負担にならない方法があるか - IPv4とIPv6で異なる設定をしなければならぬ部分が発生する可能性 - 機器ごとにデフォルトポリシーが異なると混乱する可能性がある



Oct 8,2004

IPv6PC Transition WG Home SWG

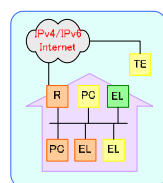
89

モデルの想定：IPv6 普及期

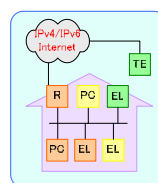
IPv6 普及期には IPv4/IPv6 を意識せずに、混在環境で利用できる状態になります。
この状態は、家庭へのリモートアクセスで、アクセスしてくる機器がどちらのプロトコルを使うかによって分類することができます。

2.3.6. モデルの想定：IPv6普及期

- IPv4と共存しつつ、IPv4/IPv6を意識しない状態へ
 - K：リモートのアクセス元がIPv4機器
 - K'：リモートのアクセス元がデュアルスタック機器 (IPv4利用)
 - L：リモートのアクセス元がIPv6機器
 - L'：リモートのアクセス元がデュアルスタック機器 (IPv6利用)



モデルK



モデルL

Oct 8,2004

IPv6PC Transition WG Home SWG

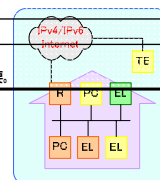
90

モデル K では、モデル H に加え、IPv4 で宅外から家庭内 LAN にリモートアクセスしてくるケースです。トランスレータ機能は、ルータ上への実装が推奨されます。

2.3.6. モデルの想定：IPv6普及期 (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IPv4機器	
説明	宅内にPC/機器が複数台、デュアルスタック、IPv4のみ、IPv6のみの機器が混在する 外部機器はIPv4を利用	
構成	ネットワークとの境界	ルータ (デュアルスタック) 接続
	接続機器	PC・ゲーム機・non-PC機器 (AV・家電機器、IPカメラ、IP電話) 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	次のいずれかの方法でグローバルプレフィックスを取得 ■ DHCPv6-PD、DTCPPなどによりISPから取得 (/48、/64が割り当てられる) ■ 自動トンネルプロトコルによる生成 ■ 静的割り当て ■ ISPから直接RAを受ける
	ローカル側	RAでプレフィックスを通知する リンクローカル
ネーミング	クエリ	Hと同じ
	登録	
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 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K



Oct 8,2004

IPv6PC Transition WG Home SWG

91

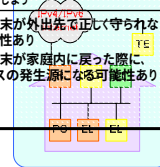
セキュリティに関しては、リモートアクセスにより生まれる新たなセキュリティ上の脅威への対策が必要となります。

2.3.6. モデルの想定:IPv6普及期 (モデルKの特徴)



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	実装度合い、方式ともにOS、機器・アプリに依存する ■ IPsec ■ SSL ■ 独自などの方式 または実施していない	■ ルーター ■ IPsecの終端 (トンネル、トランスポートモード) ■ IPsecなどのパススルー ■ エンドノード ■ IPsec, SSL, 独自方式を機器・アプリで個別に対応 ■ ルーターがエンドノードの肩代わりをできる場合はそれを使用するケースがある	◆ 遠隔端末のための進入経路が脆弱性に繋がる恐れ ■ 暗号化キーの漏洩など
	不正アクセス対応	■ ルーター対策済み ■ ただし実施はユーザに依存 ■ エンドノードはユーザに依存	■ ルーター ■ パケットフィルタ ■ エンドノード ■ パーソナルファイアウォール	◆ 遠隔端末のための進入経路が脆弱性に繋がる恐れ ■ 適切なパスワード管理、認証方法が必要 ◆ 遠隔アクセスを目的としたトランスレータの設置が脆弱性を導入する可能性があるIPv4でアクセスできなかった部分にアクセスできてしまう
	ウィルス対策	■ ウィルスチェッカーがIPv6 対応していることが望まれる ■ ISPによるウィルスチェックがIPv6対応することが望まれる	■ ルーター ■ ウィルスチェッカー (通過するパケットに対して) ■ エンドノード ■ ウィルスチェッカー ■ ISPのサービス	◆ 遠隔端末が外出先で正しく守られない可能性あり ◆ 遠隔端末が家庭内に戻った際に、ウィルスの発生源になる可能性あり

モデルK



Oct 8,2004

IPv6PC Transition WG Home SWG

92

モデル L では、リモートアクセスが IPv6 で行われます。

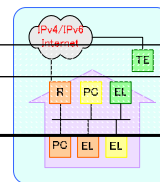
2.3.6. モデルの想定:IPv6普及期 (モデルLの特徴)



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IPv6機器	
説明	宅内にPC/機器が複数台、デュアルスタック、IPv4のみ、IPv6のみの機器が混在する 外部機器はIPv4を利用	
構成	ネットワークとの境界	ルーター(デュアルスタック)接続
	接続機器	PC・ゲーム機・non-PC機器 (AV・家電機器、IPカメラ、IP電話) IPv6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	次のいずれかの方法でグローバルプレフィックスを取得 ■ DHCPv6-PD、DTCIPなどによりISPから取得 (/48、/64が割り当てられる) ■ 自動トンネルプロトコルによる生成 ■ 静的割り当て ■ ISPから直接RAを受ける
	ローカル側	RAでプレフィックスを通知する リンクローカル
ネーミング	クエリ	Hと同じ
	登録	
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 宅内の機器一覧をどう取得するかがポイント	

(基本的にはモデルKと同じ)

モデルL



Oct 8,2004

IPv6PC Transition WG Home SWG

93

セキュリティに関しては、ここでもリモートアクセスしてくる端末への対応が必要となります。

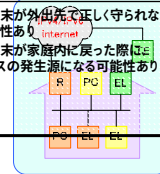
2.3.6. モデルの想定:IPv6普及期 (モデルLの特徴)



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	- 実装度合い、方式ともにOS、機器・アプリに依存する - IPsec - SSL - 独自などの方式 - または実施していない	- ルーター - IPsecの終端 (トンネル、トランスポートモード) - IPsecなどのパストルー - エンドノード - IPsec, SSL, 独自方式を機器・アプリで個別に対応 - ルーターがエンドノードの肩代わりをできる場合はそれを使用	- 遠隔端末のための進入経路が脆弱性に繋がる恐れ - 暗号化キーの漏洩など
	不正アクセス対応	- ルーター対策済み - ただし実施はユーザに依存 - エンドノードはユーザに依存	- ルーター - パケットフィルタ - エンドノード - パーソナルファイアウォール	- 遠隔端末のための進入経路が脆弱性に繋がる恐れ - 適切なパスワード管理、認証方法が必要 - 遠隔アクセスを目的としたトランスレータの設置が脆弱性を導入する可能性がある IPv4でアクセスできなかった部分にアクセスできてしまう
	ウィルス対策	- ウィルスチェッカーがIPv6 対応することが望まれる - ISPによるウィルスチェックがIPv6 対応することが望まれる	- ルーター - ウィルスチェッカー (通過するパケットに対して) - エンドノード - ウィルスチェッカー - ISPのサービス	- 遠隔端末が外出先で正しく守られない可能性あり - 遠隔端末が家庭内に戻った際には、ウィルスの発生源になる可能性あり

(基本的にはモデルKと同じ)

モデルL



Oct 8,2004

IPv6PC Transition WG Home SWG

94

モデルの想定：Non-PC モデル

IPv6 への移行に関して、家庭セグメントに特有の形態があります。それは家庭内に PC がなく、Non-PC 機器のみが繋がれている世界の移行です。

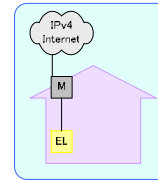
下の図で、A は現状の例です。J はデュアルスタックで特定の家電サービスを利用するような形態です。J' として、プロトコルは IPv6 のみですが、特定の家電サービスのみを利用する場合が考えられます。M は家庭内で複数の Non-PC 機器が接続されていて、これらが IPv6 に対応している形態です。O は Non-PC 機器に対する IPv6 端末からの遠隔アクセスで、O' としてデュアルスタック機器からの遠隔アクセスが考えられます。

2.3.7. モデルの想定 : non-PCモデル

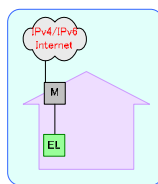


■ ホームセグメントで考えておかなければならない環境

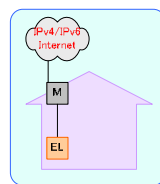
- A: 現状
- J: デュアルスタック家電お任せパック
- J': IPv6 家電お任せパック
- M: IPv6家電機器の台頭。PCをもたない家庭
- O: 遠隔アクセス (IPv6端末からの遠隔アクセス)
 - O': 遠隔アクセス (デュアルスタックからの遠隔アクセス)



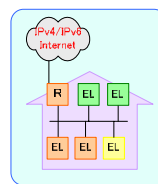
モデルA



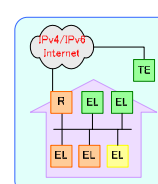
モデルJ



モデルJ'



モデルM



モデルO

Oct 8, 2004

IPv6PC Transition WG Home SWG

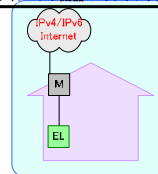
95

モデル J は、家庭内にデュアルスタックあるいはIPv6 のみに対応した Non-PC 機器が 1 台だけ存在しているというものです。インターネット側との接続は、モデムあるいはメディアコンバータによるブリッジ接続となります。家電とセットされた特定のサービスのためにネットワーク接続を利用するケースです。

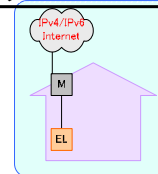
2.3.7. モデルの想定 : non-PCモデル・BCP (モデルJ)の特徴



モデル	J, J' : 家電お任せパック	
説明	宅内にデュアルスタック (モデルJ) 家電機器 / IPv6家電機器 (モデルJ') が1台	
構成	ネットワークとの境界	モデム、メディアコンバータ (ブリッジ接続)
	接続機器	デュアルスタック対応家電 (モデルJ) / IPv6家電 (モデルJ')
利用アプリ	電話、ビデオ予約、IP放送	
アドレス	インターネット側	ISPから直接RAを受ける (その他の方法も考えるが家電機器なのでRAが最も単純に対応できる)
	ローカル側	-
ネーミング	クエリ	ISPに指定されたDNSサーバ、外部からはDDNS利用
	登録	外部向け: DDNSやベンダー提供の専用サーバを利用する (IP電話の場合には、ベンダまたはキャリアが提供するSIPサーバを利用する)
設定方法	サービス提供会社がセットアップサービスを提供する可能性が高い	
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 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	



モデルJ'



モデルJ

Oct 8, 2004

IPv6PC Transition WG Home SWG

96

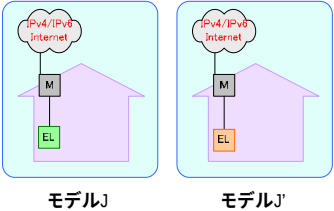
モデル J のセキュリティについては、家電製品の寿命が長いことを考えれば、認証機能を実装

しないのは危険であるなどが指摘できます。

2.3.7. モデルの想定：non-PCモデル・BCP（モデルJの特徴）



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	機器に依存	- IPsec, SSL, 独自方式を機器・アプリで個別に対応 - 通信相手ごとに対応が変化	- エンドノードでどの程度対応できるか - 薄利なノードではハードウェア暗号化は困難 - 暗号化実装自体に脆弱性があると対応が困難 (特にハードウェア)
	不正アクセス対応	機器、ユーザに依存	- 認証 - ユーザ認証 - サーバ認証 - クライアント認証 - アクセス制限 - アドレスベース - ドメイン名ベース	[対策を施していない機器の場合] IPv6で攻撃されるリスクが無いと考えられている - 機器の寿命を考えると認証機能を有していないのは危険
	ウィルス対策	対策されていない		家電機器に対するリスクが無いと考えられている



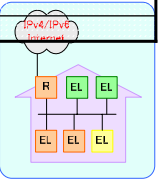
モデル J の発展型が、下表のモデル M です。接続される Non-PC 機器が複数になっており、デュアルスタック対応ルータでインターネット接続されます。名前解決では、UPnP あるいはマルチキャスト DNS などが使われます。

2.3.7. モデルの想定：non-PCモデル：夜明け前（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IPv4のみに対応し、一部はIPv6のみに対応する。ルータ(デュアルスタック)が必要になる	
構成	ネットワークとの境界	ルータ(デュアルスタック)接続
	接続機器	ゲーム機・non-PC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	次のいずれかの方法でグローバルプレフィックスを取得 - DHCPv6-PD, DTCPPなどによりISPから取得 (/48, /64が割り当てられる) - 自動トンネルプロトコルによる生成 - 静的割り当て - ISPから直接RAを受ける
	ローカル側	RAでプレフィックスを通知する リンクローカル
ネーミング	クエリ	UPnPやマルチキャストDNSなど
	登録	宅内に閉じたDNSサーバ相当の機能を持つノード、命名方法に課題あり
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M



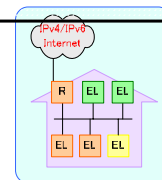
セキュリティに関しては、たとえば通信の暗号化が必要となりますが、家電のみの世界であるため、煩雑さを伴わない実装が求められます。

2.3.7. モデルの想定：non-PCモデル・夜明け前（モデルMの特徴）



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	- 実装度合い、方式ともに機器・アプリに依存する ■ IPsec ■ SSL ■ 独自などの方式または実施していない	■ ルータ ■ IPsecの終端（トンネル、トランスポートモード） ■ IPsecなどのパススルー ■ エンドノード ■ IPsec, SSL, 独自方式を機器・アプリで個別に対応 ■ ルータがエンドノードの肩代わりができる場合はそれを使用するケースがある	◆ 遠隔端末のための進入経路が脆弱性に繋がる恐れ ■ 暗号化キーの漏洩など ■ 家電のみのため、適切且つ平易な暗号設定方法が必要
	不正アクセス対応	■ ルータ対策済み ■ ただし実施はユーザに依存 ■ エンドノードはユーザに依存	■ ルータ ■ パケットフィルタ ■ エンドノード ■ パーソナルファイアウォール ■ 各種認証	■ 家電のみのため、適切な設定方法が必要
	ウィルス対策	■ ISPのサービスやASPのサービスに期待 ■ エンドノードにもウィルス対策がされることを期待	??	■ 家電機器に対するウィルスの脅威がはっきりしていない

モデルM



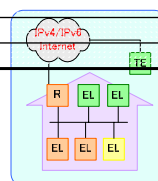
さらに進展すると、H の状況に加え、外部から IPv4 で家庭内機器にアクセスする機器が登場します。トランスレータ機能はルータに実装することが推奨されます。

2.3.7. モデルの想定：non-PCモデル・IPv6普及期（モデルQの特徴）



モデル	O：Hの状況+リモートから宅内機器にアクセスするIPv4機器	
説明	宅内に機器が複数台、デュアルスタック、IPv4のみ、IPv6のみの機器が混在する外部機器はIPv6を利用	
構成	ネットワークとの境界	ルータ（デュアルスタック）接続
	接続機器	ゲーム機・non-PC機器（AV・家電機器、IPカメラ、IP電話） IPv6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	次のいずれかの方法でグローバルプレフィックスを取得 ■ DHCPv6-PD、DTCPPなどによりISPから取得（/48、/64が割り当てられる） ■ 自動トンネルプロトコルによる生成 ■ 静的割り当て ■ ISPから直接RAを受ける
	ローカル側	RAでプレフィックスを通知する リンクローカル
ネーミング	クエリ	Hと同じ
	登録	家電機器のみであるため、注意が必要
設定方法	トランスレータへの設定に関しては別途考察が必要	
その他	トランスレータ機能はルータ上への実装を推奨	

モデルO



Oct 8,2004

IPv6PC Transition WG Home SWG

100

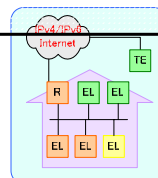
セキュリティに関しては、通信の暗号化もさることながら、不正アクセスの防止機能を強化しなければなりません。

2.3.7. モデルの想定：non-PCモデル・IPv6普及期（モデルQの特徴）



セキュリティ対策	対策項目	対策状況	対策方法	脅威、問題点など
	暗号化	実装度合い、方式ともに機器・アプリに依存する ■ IPsec ■ SSL ■ 独自 などの方式 または実施していない	■ ルータ ■ IPsecの終端（トンネル、トランスポートモード） ■ IPsecなどのパススルー ■ エンドノード ■ IPsec、SSL、独自方式を機器・アプリで個別に対応 ルータがエンドノードの肩代わりをできる場合はそれを使用するケースがある	◆ 遠隔端末のための進入経路が脆弱性に繋がる恐れ ■ 暗号化キーの漏洩など ■ 家電のみのため、適切且つ平易な暗号設定方法が必要
	不正アクセス対応	■ ルータ対策済み ■ ただし実施はユーザに依存 ■ エンドノードはユーザに依存	■ ルータ ■ パケットフィルタ ■ エンドノード ■ パーソナルファイアウォール ■ 各種認証	◆ 遠隔端末のための進入経路が脆弱性に繋がる恐れ ■ 暗号化キーの漏洩など ■ 家電のみのため、適切な設定方法が必要
	ウィルス対策	■ ISPのサービスやASPのサービスに期待 ■ エンドノードにもウィルス対策がされることを期待	??	■ 家電機器に対するウィルスの脅威がはつきりしていない

モデルQ



Oct 8,2004

IPv6PC Transition WG Home SWG

101

現状から BCP への移行ポイント

以上を総合すると、現在の状態から BCP に移行する際には、次のような点をフォローする必要があります。

構成

できればルータ利用の形態へ誘導する

IPv6 ブリッジ機能を利用する場合には、エンドノードのセキュリティ確保をユーザに促す

パーソナルファイアウォールの利用を強く推奨

RA Proxy 機能を搭載した製品がセキュリティ上推奨される

アプリケーション

BCP 段階では、魅力的な IPv6 アプリの提供が望まれる

ユーザは v4 で満足している

IPv6 を利用する IP 電話、マルチキャスト放送が普及すれば、弾みがつくかも

現状の IPv4 アプリは IPv4 のまま使われ続ける

アドレス・ネーミング

IPv4 と併用する

DNS のトランスポートプロトコルとしては、IPv4 を中心に利用する

セキュリティ

暗号化 (IPsec、PPTP(?)) はルータで実施

SSL、アプリケーションレベルの暗号化も継続利用

パーソナルファイアウォール (市販製品) の IPv6 対応を期待

その他

Non-PC な機器への各種設定方法・自動化が望まれるが、現状から BCP への移行段階では困難

家庭内通信方式の検討は IPv4 が先行しており、BCP 環境でも IPv4 が有力である

Non-PC 主導の移行シナリオについて

Non-PC のみの環境の移行においても、基本的には、PC が主導の移行シナリオと同様の課題を抱えています。

Non-PC ならではの条件としては、下記のような点が挙げられます。

- ・セキュリティ機能はルータに期待

(小型ノードでの実装はノード単価の上昇を招く可能性がある、小型ノードでは余計なパケットは処理したくない、消費電力の増加、レスポンス性能の低下、などにつながるため)

- ・現状では、PC (ブラウザ機能) がないと、non-PC の設定もルータの設定もできない

デジタルTVなどが搭載するブラウザ機能の利用を図る。この際 HTML の互換性に十分注意する必要がある。HTML 中のスクリプトの使用に関しても注意する必要がある)

- ・自動設定機能の普及が必要

アクセス網／ISP 主導によるモデム、ルータなどの設定自動化が必要

3. プレイヤーにおける移行シナリオ

サービス移行シナリオからの導入

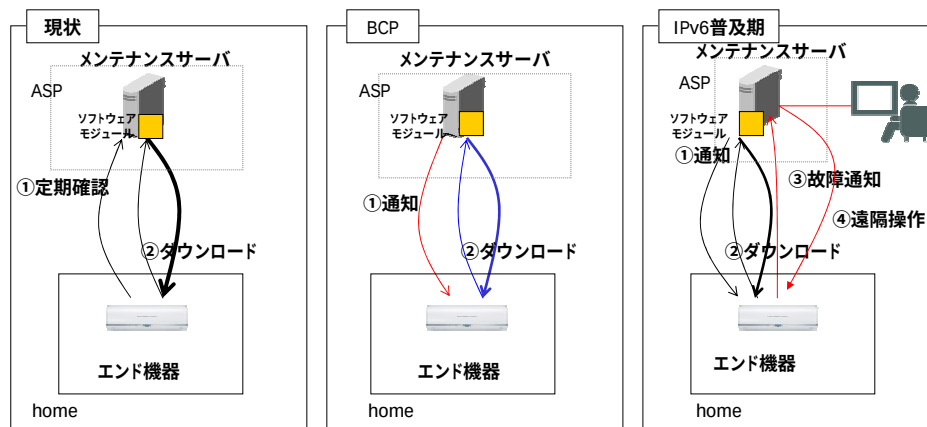
ここでは具体的なサービス(想定シナリオ)を想定し、プレイヤーにおける移行シナリオを導入します。ここでは遠隔メンテナンスとネットワークゲームについて検討します。

遠隔メンテナンスシナリオ

3.1.1. 遠隔メンテナンスシナリオ



■ 遠隔メンテナンスにおけるサービスイメージ図



Oct 8,2004

IPv6PC Transition WG Home SWG

107

ここでは、あるエンド機器に対する、よりタイムリーで確実な遠隔メンテナンスの実施を考えます。現状では、エンド機器自体がソフトウェア更新を自らネットワーク経由でチェックし、更新があった場合には、これをダウンロードしてインストールするという方法がとられているとします。

より確実で迅速なアップデートを実現するため、ソフトのアップデートモジュールが提供可能になると、メンテナンスサーバ側からエンド機器に対してこれを通知する仕組みに移行します。エンド機器はこれを受けて、アップデートモジュールをダウンロードすることになります。

さらに IPv6 普及期には、エンド機器から故障の通知を受けて、保守スタッフがエンド機器を遠隔操作して対応作業を実施する仕組みに移行します。

3.1.1. 遠隔メンテナンスシナリオ



■ 遠隔メンテナンス シナリオ

■ シナリオ機能概略

■ 現状

- エンド機器は定期的にメンテナンスサーバに対してソフトウェアモジュールがアップデートされていないか確認する
- アップデートされていた場合には、ユーザが操作を行いソフトウェアモジュールをダウンロードして入れ替える

■ BCP

- メンテナンスサーバは、アップデートされたソフトウェアモジュールがあるとエンド機器に対して通知を行う
- エンド機器は、その通知を受取ると自動的にソフトウェアモジュールをダウンロードして入れ替える

■ 5.5

- エンド機器から故障通知があると、保守員がエンド機器を遠隔から操作し、故障原因を分析しそれに対する対処を行う

このシナリオでは、サービス提供者、ユーザの双方にとって下記のようなメリットが考えられます。

3.1.1. 遠隔メンテナンスシナリオ



■ 遠隔メンテナンス シナリオ

■ シナリオに対するサービス提供者/ユーザのメリット

■ 現状

- サービス提供者: ソフトウェアのメンテナンスコストが下がる
- ユーザ : 最新のソフトウェアが使用できる

■ BCP

- サービス提供者: サーバ負荷をコントロールでき運用コストが低減できる
- ユーザ : 最新のソフトウェアが自動的にインストールされ、早期に使用できる。

■ IPv6普及期

- サービス提供者: 保守員を現地に派遣するコストが削減できる
- ユーザ : 故障がいち早く発見され修理されるので、機器が使用できない期間が短くなる

このシナリオにおけるサービスの実行形態を分類すると、下記ようになります。

3.1.1. 遠隔メンテナンスシナリオ



■ 遠隔メンテナンスにおけるサービス分類

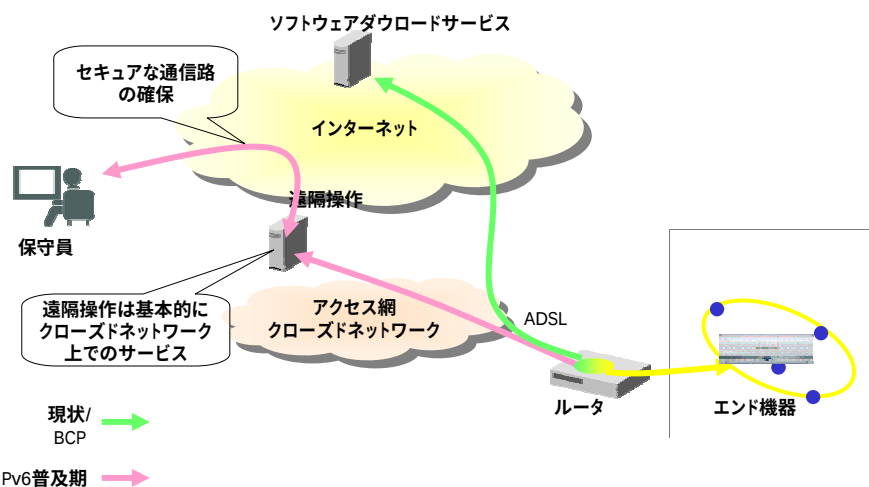
- 現状
 - 定期的な確認 (F)Client/Server (クライアントポスト) 型
 - ソフトウェアのダウンロード (D)Client/Server型
- BCP
 - 定期的な確認 (E)Client/Server (ASPポーリング) 型
 - ソフトのアップグレード (D)Client/Server型
- IPv6普及期
 - 定期的な確認 (E)Client/Server (ASPポーリング) 型
 - ソフトウェアのダウンロード (D)Client/Server型
 - 遠隔操作 (D)Client/Server型 + (F)Client/Server (クライアントポスト)

ネットワーク的には、アップデートモジュールの提供／取得はオープンなネットワーク上で行いますが、IPv6 普及期に行われる遠隔操作については、クローズドなネットワーク経由で実施します。

3.1.1. 遠隔メンテナンスシナリオ



■ ネットワーク構成



現状

このシナリオにおける現状では、メンテナンスにおける通信はすべて IPv4 によって行われ、常に家庭のエンド機器側が通信を開始します。

この段階における各プレイヤーの状況については、後述の「プレイヤーにおけるシナリオ」の該当箇所をご覧ください。

3.1.1. 遠隔メンテナンスシナリオ



■ 現状

■ 特徴

- IPv4での通信
- 通信は、ホームが発信元

■ 各プレイヤー関係箇所へのリンク

- エンド機器提供者
 - 組込機器編:現状
- ネットワーク機器提供者
 - L3以上機器 (複合機器含む) 編 現状
- 通信ネットワーク (全般)
 - ISP SWG
- サービス提供者
 - (D)Client/Server型:現状
 - (F)Client/Server (クライアントポスト) 型:現状

BCP

BCP では、IPv6 を利用します。IPv6 を使うことで、外部から家庭に対して任意に通知を行うことが可能になります。ただし、セキュリティ上の配慮が新たに必要となります。

3.1.1. 遠隔メンテナンスシナリオ



■ BCP

- 特徴
 - IPv6での通信
 - 外からホームへの通信が発生
 - セキュリティの考慮が必要
- 各プレイヤー関係箇所へのリンク
 - エンド機器提供者
 - 組込機器編: BCP
 - ネットワーク機器提供者
 - L3以上機器 (複合機器含む) 編 BCP
 - 通信ネットワーク提供者
 - ISP SWG
 - サービス提供者
 - (D)Client/Server型: BCP
 - (E)Client/Server (ASPポーリング) 型: BCP
 - その他
 - セキュリティSWG

Oct 8, 2004

IPv6PC Transition WG Home SWG

113

IPv6 普及期

IPv6 普及期には、IPv6 を活用し、外から家庭に対して通知をするだけでなく、エンド機器の遠隔的な操作を行うことになります。この段階では厳格なセキュリティ対策が求められます。

3.1.1. 遠隔メンテナンスシナリオ



■ IPv6普及期

- 特徴
 - IPv6での通信
 - 外からホームへの通信が発生
 - ホーム内にあるエンド機器を操作するので強固なセキュリティが必要
- 各プレイヤー関係箇所へのリンク
 - エンド機器提供者
 - 組込機器編: BCP/IPv6普及期
 - ネットワーク機器提供者
 - L3以上機器 (複合機器含む) 編: BCP/IPv6普及期
 - 通信ネットワーク提供者
 - ISP SWG
 - サービス提供者
 - (D)Client/Server型: BCP/IPv6普及期
 - (E)Client/Server (ASPポーリング) 型: BCP/IPv6普及期
 - (F)Client/Server (クライアントポスト) 型: BCP/IPv6普及期
 - その他
 - セキュリティSWG

Oct 8, 2004

IPv6PC Transition WG Home SWG

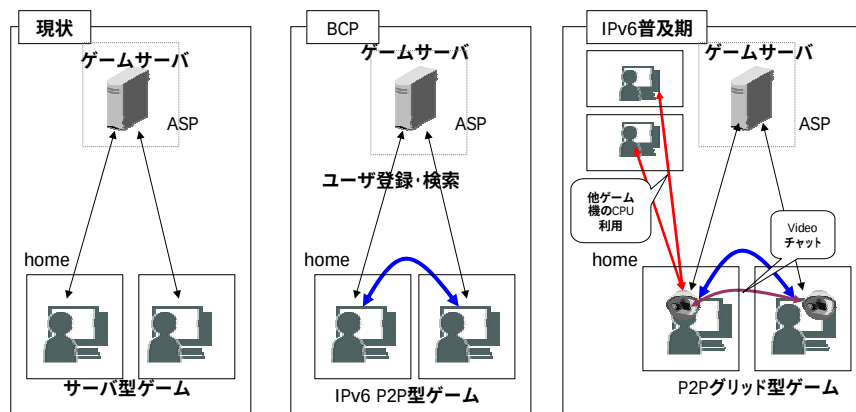
114

ネットワークゲームシナリオ

3.1.2. ネットワークゲームシナリオ



■ ネットワークゲームにおけるサービスイメージ図



Oct 8, 2004

IPv6PC Transition WG Home SWG

115

これは、ネットワークゲームの機能を強化していくシナリオです。現状のネットワーク対戦ゲームはゲームの全機能がサーバによって制御されています。BCP としては、サーバによってユーザの登録や管理は実行するものの、実際の対戦はユーザのエンド端末間の直接通信によって行うピアツーピア (P2P) 型のゲームを提供します。さらに IPv6 普及期においては、リアルタイムのビデオチャットなどのアプリケーションを展開するとともに、ネットワーク接続されている他のエンド機器の余っている CPU サイクルを活用することで、より負荷の高いゲームを可能にするグリッドコンピューティングの実現を図ります。

3.1.2. ネットワークゲームシナリオ



■ ネットワークゲーム シナリオ

■ シナリオ機能概略

- 現状
 - サーバを介してユーザ間の通信を行いゲームを家庭間で実行する
- BCP
 - サーバ側でユーザの登録・検索を提供し、P2P型ゲームを家庭間で実行する
- IPv6普及期
 - P2P型ゲームにおいて、Videoチャットのようなリアルタイムな映像コンテンツを家庭間で利用する
 - ゲームにおいて多大なCPUリソースを使用する場合、グリッド機能によって他ゲーム機のCPUを家庭間で利用する。

Oct 8,2004

IPv6PC Transition WG Home SWG

116

このシナリオでは、サービス提供者にとって新しい形態のゲームを、より低いコストで提供するチャンスを与えるとともに、ユーザにとっても、これまで実現しにくかった種類のゲームを楽しめる可能性を提供します。

3.1.2. ネットワークゲームシナリオ



■ ネットワークゲーム シナリオ

■ シナリオに対するサービス提供者/ユーザ側のメリット

- 現状
 - サービス提供者:サーバ介した新しい形態のゲームの提供ができる
 - ユーザ :他ユーザと協力してゲームが楽しめる
- BCP
 - サービス提供者:サーバ負荷を抑えることができ投資の抑制になる
 - ユーザ :サーバの混雑を回避できかつ他ユーザと協力してゲームが楽しめる
- IPv6普及期
 - サービス提供者:CPU処理の高いゲームの提供と映像コンテンツを利用する新規のゲームが提供できる
 - ユーザ :新しい形態のゲームが利用できる

Oct 8,2004

IPv6PC Transition WG Home SWG

117

このシナリオにおいて、ネットワークゲームのネットワーク利用形態は、下記のように進化していきます。

3.1.2. ネットワークゲームシナリオ



■ ネットワークゲームにおけるサービス分類

■ 現状

- サーバ型ネットワークゲーム (D)Client/Server型

■ BCP

- サーバ型ネットワークゲーム (D)Client/Server型
- P2P型ネットワークゲーム (C)P2P+ロビーサーバ型

■ IPv6普及期

- サーバ型ネットワークゲーム (D)Client/Server型
- P2P型ネットワークゲーム (C)P2P+ロビーサーバ型
 - P2PVideoチャット機能の追加
- グリッド型ネットワークゲーム (B)P2P+接続管理サーバ

Oct 8,2004

IPv6PC Transition WG Home SWG

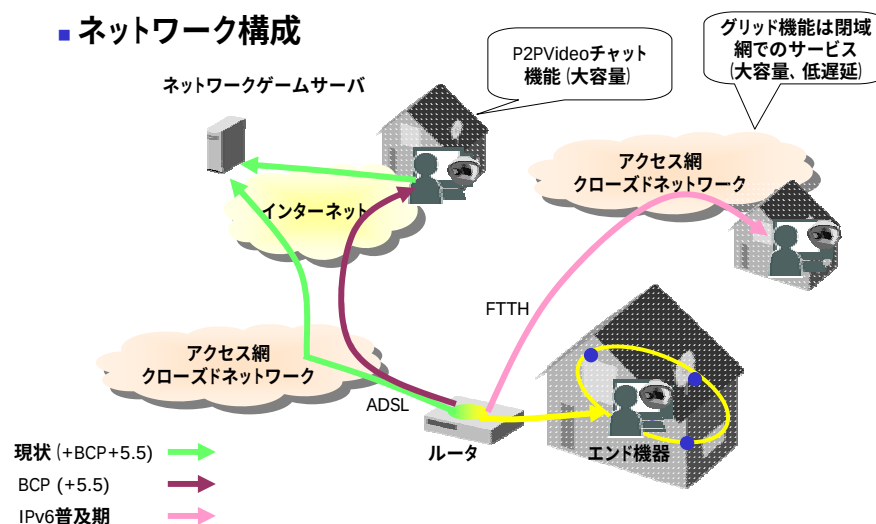
118

ネットワーク的には、オープンなネットワーク上でビデオチャットなどの大容量通信が増加していくほか、クローズドなネットワークで、大容量と低遅延を生かしたグリッドコンピューティングが行われるようになります。

3.1.2. ネットワークゲーム シナリオ



■ ネットワーク構成



Oct 8,2004

IPv6PC Transition WG Home SWG

119

現状

現状のネットワークゲームは IPv4 による通信に基づいており、通信を開始するのは必ず家庭側のエンド機器です。各プレイヤーの状況は、後述の「プレイヤーにおけるシナリオ」中の下記の該当箇所に示されています。

3.1.2. ネットワークゲーム シナリオ



■ 現状

■ 特徴

- IPv4
- 通信は、ホームが発信元
- 各プレイヤー関係箇所へのリンク
 - エンド機器提供者
 - 組込機器編:現状
 - ネットワーク機器提供者
 - L3以上機器 (複合機器含む) 編:現状
 - 通信ネットワーク提供者
 - ISP SWG
 - サービス提供者
 - (D)Client/Server型:現状

BCP

BCP では、IPv6 による家庭間の通信が行われるようになります。これに伴って、セキュリティ機能はゲームにおける公平性を確保するためにも重要になります。さらに P2P 通信における遅延や QoS の問題への対処も必要になってきます。

3.1.2. ネットワークゲーム シナリオ



■ BCP

- 特徴
 - IPv6
 - 家庭間の通信が発生
 - ユーザ情報を守る、公平性を維持するためのセキュリティ機能
 - ネットワークの大容量化、低遅延、QoSの対応
- 各プレイヤー関係箇所へのリンク
 - エンド機器提供者
 - 組込機器編: BCP
 - ネットワーク機器提供者
 - L3以上機器 (複合機器含む) 編: BCP
 - 通信ネットワーク提供者
 - ISP SWG
 - サービス提供者
 - (B)P2P+接続管理サーバ: BCP
 - (C)P2P+ロビーサーバ型: BCP
 - (D)Client/Server型: BCP
 - その他
 - セキュリティ SWG

Oct 8,2004

IPv6PC Transition WG Home SWG

121

IPv6 普及期

この時期には、BCP における問題への対処に加え、グリッドコンピューティングのための閉域網利用とオープンなネットワーク上でのゲームの実行を両立させるため、エンド機器におけるマルチホーム／マルチプレフィックス対応が求められます。

3.1.2. ネットワークゲーム シナリオ



■ IPv6普及期

- 特徴
 - IPv6
 - 家庭間の通信が発生
 - ユーザ情報を守る、公平性を維持するためのセキュリティ機能
 - ネットワークの大容量、低遅延、QoSの対応
 - CPE、エンド機器のマルチホーム/マルチプレフィックス対応
- 各プレイヤー関係箇所へのリンク
 - エンド機器提供者
 - 組込機器編: BCP/IPv6普及期
 - ネットワーク機器提供者
 - L3以上機器 (複合機器含む) 編 BCP/IPv6普及期
 - 通信ネットワーク ISP提供者
 - ISP SWG
 - サービス提供者
 - サービス(C)P2P+ロビーサーバ型: BCP/IPv6普及期
 - サービス(D)Client/Server型: BCP/IPv6普及期
 - その他
 - セキュリティ SWG

Oct 8,2004

IPv6PC Transition WG Home SWG

122

各プレイヤーにおける移行シナリオ

冒頭部分で、家庭ネットワークの IPv6 移行にかかわるプレイヤーを分類しました。下記では、それぞれのプレイヤーにおける移行・導入手順、注意事項、問題点を整理します。移行に関して複数の選択肢が存在する場合は、そのメリットとデメリットを明確に示します。

なお、サービス提供者編については、IPv6 だけに特化したものでなく、IP を利用したもの全般に言える内容も含んでいます。

プレイヤーにおけるシナリオ：エンド機器提供者

ここでは、エンド機器を PC (OS・ミドルウェア)、PC (アプリケーション)、組み込み機器の 3 種に分類して検討します。

機器の種類ではなく、このような分類にしたのは、利用用途と機器が実現すべきネットワーク機能は必ずしも一致しないからです。ネットワーク機能は搭載 CPU の能力に大きく依存します。特に PC と組み込み機器では、ユーザーインターフェースの有無、セキュリティ機構に使用可能な計算機リソース、汎用／専用など、要求事項がかなり異なります。

さらに、PC 上の OS・ミドルウェア開発と応用アプリケーション開発では、ネットワーク層、トランスポート層プロトコルレベルの対応と、アプリケーション層レベルの対応という点で、要求が異なります。

3.2.1. プレイヤーにおける移行シナリオ (エンド機器提供者編)



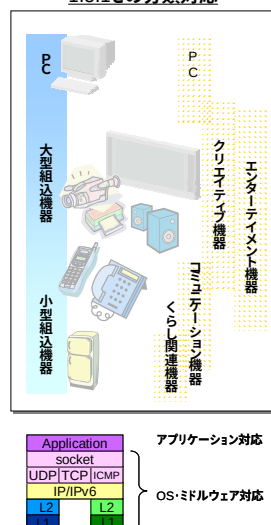
- エンド機器提供者編では、機器を分類して以下のようにまとめる

- PC (OS・ミドルウェア)
- PC (アプリケーション)
- 組み込み機器

- 分類の理由：

- 実アプリケーション分類と機器が実現すべき内容は必ずしも一致しない。
 - むしろ計算機リソースの影響を大きく受ける
- PC と組み込み機器では要求事項が異なる
 - ユーザーインターフェースの有無
 - セキュリティ機構に使用可能な計算機リソース
 - 汎用／専用
- PC 上の OS・ミドルウェア開発と応用アプリケーション開発では要求が異なる
 - ネットワーク層、トランスポート層プロトコルレベルの対応
 - アプリケーション層レベルの対応

1.3.1との分類対応



組込機器の現状

IPv6 スタックには、小型機器向けとして各種 ITRON OS、Linux、Windows CE .NET など、大型機器向けには Windows XP Embedded、CE などを対象としたものが多数存在しています。

実装に関しては、IPv6 Ready Logo プログラム (<http://www.ipv6ready.org/>) とその仕様が参考になります。

しかし、市販されている組込機器の大部分は IPv6 に対応していません。IPv4 を使った機能拡張が多数行われ、通信手順の複雑化といった弊害を生んでいたり、独自プロトコルを使った閉塞網を構成していたりします。

IPv6 対応の組み込み機器は、現在のところ数社から発売されています。ネットワークカメラ、センサー集中管理装置、IP 電話、セットトップボックス (サービス利用を前提とした一括販売が想定されている) などです。

組込機器におけるアプリケーションプロトコルは、分野により異なるのが通例です。種々の方式が議論され、採用されていますが、一本化には時間がかかります。IPv6 に特化した標準方式は存在しません。IP 対応機器では、IPv4 に対する方式を IPv6 に拡張しようという動きはあります。

組込機器の BCP

要求事項 (必須)

組込機器に必須の要求事項は、以下の通りです。

1.スタックの IPv6 対応 (デュアルスタック化)

開発済み IPv6 スタックの購入、特定 OS 用に新規開発、の 2 つの選択肢があります。

必須要件としては、IPv6 の基本プロトコル (IPv6 Ready Logo Phase-1 に示されたアドレス自動設定 (NDP 含む) やパケット送受信の仕様) を実装していればよく、I-D (draft-ietf-ipv6-node-requirements)、TACA Project (www.taca.jp) が参考になります。

2.ユーザーインターフェース

IPv6 関連情報の表示と設定ができるようにすべきですが、基本は プラグ・アンド・プレイです。

3.適切なアプリケーションの作りこみ

アドレスファミリー独立なプログラミング (ソケット、アドレスなど)、通信の受信アドレスや送信アドレスの適切な決定 (使い勝手が下がらないように) などが重要です。IPv6 利用不可能時にスムーズなフォールバックを実現する必要もあります。

4.名前解決

名前解決では、次のような対策が求められます。

DNS クエリ AAAA レコード対応

DNS トランスポートの IPv6 対応は不要 (デュアルスタック時)

DDNS 登録 登録プロトコルの AAAA レコード対応

(DDNS サーバ側の AAAA レコード対応)

その他 ベンダー独自実装 (→標準化への働きかけが望まれる)

5.セキュリティ機構

アクセス制限

方式としては、ユーザ／パスワード認証、ノード (Unique ID) ベース、アドレスベース、ドメイン名ベースが考えられます。

IPv4 Mapped Addressに対応しているスタックの場合は注意が必要です。IPv6 ソケットを使ってIPv4 接続が確立してしまう可能性があります。また、逆引きに基づくアクセス制限は利用できないか、利用すべきではありません。

方法としては、アプリケーションレベルの作りこみか、組み込み機器レベルでの対応となります。ただし、ユーザーインターフェースがないとセキュリティ機構の設定が困難という問題が残ります。事前に適当なポリシーを決めてしまう方法 (同一プレフィックスのみ許可、など) や、物理的に解決する手段 (近接デバイス認証、赤外線通信との併用など) もありえます。

方式や方法は、開発機器の特性に合わせて選択する必要があります。

要求事項 (オプション)

[安全な通信を実現したい]

安全な通信を実現する手段としては、IPsec 対応と SSL 対応があります。

IPsec の実装には、ソフトウェア対応とハードウェア対応があります。

ソフトウェア対応のメリットは安価だということで、デメリットとしては、パフォーマンスの低下、脆弱性の導入に繋がる恐れが指摘されます。

ハードウェア対応のメリットは良好なパフォーマンスです。デメリットは高価で、OS/プロトコルスタックに手を加える必要があるという点にあります。

IPsec 全体のデメリットは、IKE、IKEv2、スタティックなど、鍵交換のための仕組みが別途必要で、IKE の初期設定問題が残ります。また、Windows XP (SP2 含む) の IPv6 IPsec スタックは、暗号化のための ESP を使用できません。

一方、SSL 対応のメリットは、対応クライアントが豊富 (Web ブラウザが利用可能) だということ

で、デメリット TCP ベースのアプリケーションしか使えないということにあります。

[設定を自動化したい]

NDP (アドレス設定、デフォルトルータ設定) 以外の自動化は標準化されていないため、独自方式を実装する必要があります。独自方式の実装で利便性の向上というメリットがありますが、ベンダー独自方式のため相互接続性が悪くなるというデメリットが生じます。

[IPv6 ルータがない場合でも IPv6 を使いたい]

[アクセス回線が IPv6 をサポートしていなくても IPv6 を使いたい]

これらの要求に応えるには、IPv6 終端機能を実装する必要があります。方法としては、トンネルで終端、あるいはアクセス回線を終端、の 2 通りがあります。全体的なデメリットとして、単一機器で実装すると、計算機リソースを圧迫する可能性が大きい点が挙げられます。

・トンネルで終端

この場合、アクセス回線の終端は既存終端装置 (ルータなど) を利用し、IPv4 上に IPv6 トンネルを確立して利用します。メリットとしては、アクセス回線の IPv6 化が必ずしも必要ないということです。機器の製造・販売元がトンネルサーバ／ASP を兼用することも可能です。デメリットは、トンネル方式が乱立しており、デファクトと呼べるものがないということです。トンネル接続提供者ごとに方式が異なるため、実装が困難であり、トンネルを利用することで IPv4 と IPv6 の接続性に違いが発生します。これがユーザビリティを低下し、ユーザを混乱させる可能性が大きいほか、実装コストも増加します。

・アクセス回線を終端

アクセス終端装置に機能を組み込む (組み込み、後付オプション、など) ことが考えられます。メリットは確実に IPv6 通信が利用できることですが、デメリットとして高コストになることが指摘できます。やはりアクセス回線の IPv6 化が前提となります。

[GUI で設定操作を行いたい]

[プラグ・アンド・プレイ以上の詳細設定をしたい]

これには、操作部や表示部を持たない機器を考慮した汎用ユーザーインターフェースの提供や利用が考えられます。PC やデジタル TV などの Web ブラウザを利用することが選択肢となります。

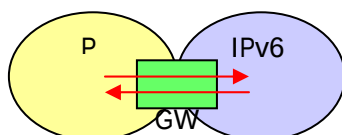
組込機器の IPv6 普及期

要求事項 (必須)

組込機器の IPv6 普及期における必須の要求事項は以下の通りです。

1. 特定アプリケーションプロトコル／ネットワークとのゲートウェイ技術の標準化

閉じたネットワークを形成するプロトコルの IPv6 網への結合が必要となります。これについては、独自プロトコル $P \rightarrow \text{IPv6}$ 、 $\text{IPv6} \rightarrow$ 独自プロトコル P の相互変換が理想です。ただし、プロトコル、アプリケーションの動作次第では片方向でもよい（センサーによる状態通知など）と考えられます。



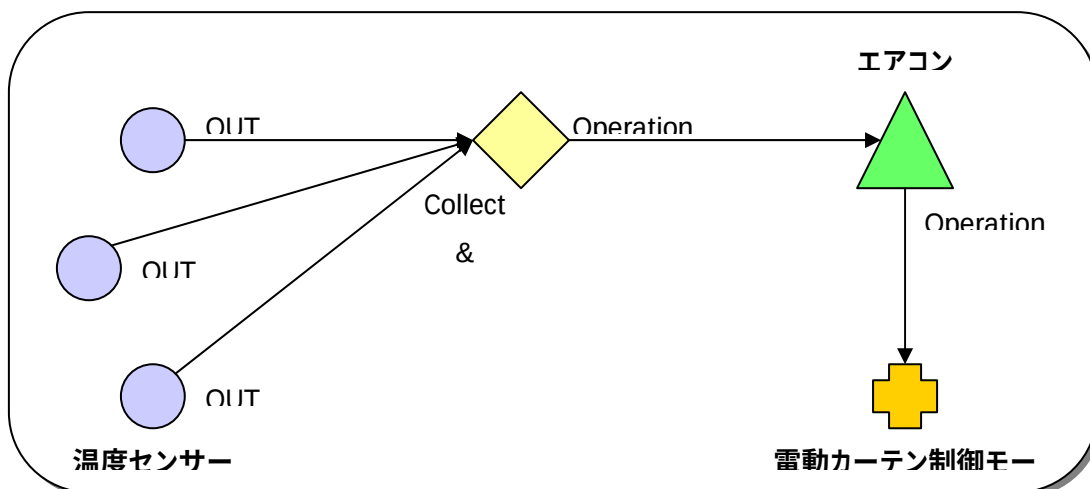
これについては、IPv6 対応アプリケーションプロトコルの標準化と併せて進めることが好ましいと考えられます。

2. IPv6 対応アプリケーションプロトコルの標準化

アプリケーションプロトコルのトランスポートを IPv6 に対応させることと、アプリケーションプロトコルで交換する情報を IPv6 に対応させることが望めます。具体的には、サービス発見／通知／制御プロトコル、その他プロトコル内部に含まれるアドレス情報があります。

3. 複数機器の柔軟な連携を実現

これには、動作シーケンス（対象となるノード、イベント、条件）の定義、運用の実現が必要となります。メリットは、複数機器を連携させることで、高度な機能が実現できるということです。つまり、異種ベンダー間での連携を実現することで、ISP やベンダーからの一括制御なども可能となり、利便性が向上します。デメリットは、標準機構が存在しないため、囲い込みが発生する恐れがあることです。一方、標準化作業に伴う問題解決の遅延も危惧されます。



4.セキュリティ強化

セキュリティに関しては、すべての機器が同列に対応することはできません。

・自ノードで対応可能な場合

この場合、IPsec、SSL、動的鍵交換、暗号／ハッシュアルゴリズムなど、各種セキュリティ機構から適切なものを実装することになります。

・自ノードで対応できない場合

CPE（ルータ、ブリッジ）に対して適切な防御を要請する仕組みを備える必要があります。通信相手を限定して、それ以外は通信できないようにする、などの処理を加えなければなりません。

また、セキュリティ対策手法の確立が求められます。

オンラインの自動アップデートには、プッシュ式とプル式がありますが、ユーザの同意が必要となります。オフラインのアップデートは、使用契約などがある組込機器について、アップデートソフトを送付する形態です。

5.名前解決、機器発見機構

機器の一括管理や機器の一覧表示のため、家庭内に存在する複数機器の検出機構が必要となります。利用者が容易に検出、判別可能な名前付け機構が求められます（自然言語による名前付け家庭内の場所との関連づけなど）。IPv6 におけるデファクトスタンダードの登場が望まれます。

要求事項 (オプション)

[より安全な通信を実現したい]

これについては、アクセス制限手段、セキュアデータチャネル確立の手段として、Trusted 3rd Party Model などの新しいセキュリティ機構の活用が求められます。このモデルのメリットとしては設定が簡略化できます。デメリットとしては信頼を置く第三者が Single Point of Failure になる、通信を行うときに遅延が発生する、アプリケーションごとに対応が必要、ビジネス面での協業が必要（もしくはすべてを抱え込む）、が考えられます。

[機器をより安全に守りたい]

ネットワーク機器の制御、特に家庭の入り口にあるファイアウォール制御については、UPnP IGD の IPv6 対応などの制御機構の登場が期待されます。そのメリットは、通信しないときは外界から遮断できるので安全性が向上することで、デメリットは独立して外部から始まる通信をうまく扱うことができないことです。

[多くの機器を安全な状態に保ちたい]

これには家庭内のセキュリティポリシー、設定の一元管理が必要となります。メリットは、個別設定を回避することで、ミスオペレーションの可能性を減らすことができ、新たな脅威が発生した場合でも、修正が容易 (ISP やベンダーからの一括制御なども可能) ということにあります。

デメリットは、標準機構が存在しないため、困り込みが発生する恐れがあり、仮に標準化作業を行う場合でも、標準化作業に伴う問題解決の遅延が考えられるということにあります。

[プライバシーを考慮した通信を実現したい]

Private Extension に対応することで、IPv6 アドレスの下位 64 ビット (インタフェース ID) は動的に変更できます。それ以上の通信の秘匿性を実現することは、現状では困難です。しかし、これについては、研究レベルでいくつかの提案がなされているので、今後の技術展開、標準化が期待されます。サーバ側、ユーザ側双方が通信主体の秘匿性を保ったまま暗号化する方法などが研究されています。

PC (OS・ミドルウェア) の現状

すでに Windows シリーズ、Mac OS X、Linux、BSD 系 OS、Solaris など、大部分の OS は IPv6 対応を完了しています。

基本的な相互接続性は確保されていますが、相違点も存在します。主要な相違点は以下の通りです。

- ・Advanced API の実装
- ・実装ごとに異なるレゾルバの挙動
- ・Node Information Query の実装
- ・Privacy Extension の実装と送信元アドレスの決定方法
- ・DNS の IPv6 トランスポート
- ・DNS UPDATE
- ・IPsec

OS の IPv6 実装には、接続までに時間がかかる、接続できないなど、問題点も指摘されています。(WIDE プロジェクトで IPv6 Fix という活動が開始されています。 <http://www.v6fix.net/>)

また、OS の初期状態における IP の有効・無効は OS によって違います。Mac OS X は有効、Windows 無効で、Linux はディストリビューションごとに異なっています。

PC (OS・ミドルウェア) の BCP

IPv6 を有効にすれば原則として使用可能であり、根本的な対応は必要ありません。

ただし、ウイルス対策ソフトウェア、パーソナルファイアウォール、DNS／レゾルバ、アプリケーションなどに問題があります。

ウイルス対策ソフトウェアの問題

ウイルス対策ソフトウェアのうち、ネットワークプロトコルを解析するタイプは IPv6 未対応です (2004/10/01 現在)。

(例) IPv6 POP3 経由でメールを読むと、ウイルスチェックが行われない
ディスクに書き込みが発生する時点で初めて検出される

パーソナルファイアウォールの問題

パーソナルファイアウォールは IPv6 に未対応です (パッケージ製品、2004/10/01 現在)。
Windows XP (SP1+Advanced Network Pack、SP2) の IPv6 ファイアウォールはステートフル動作が可能ですが、GUI はありません。

DNS/レゾルバ問題

DNS サーバが CNAME や A レコードを返しているにもかかわらず、処理しないスタックが存在します。

アプリケーション問題

IPv6 接続性がないネットワークでも、DNS の応答で AAAA が得られると、無条件に IPv6 接続を試みてしまうという問題があります。IPv4 へのフォールバックが完全ではなく、時間がかかるケースが報告されています。

PC (OS・ミドルウェア) の IPv6 普及期

要求事項 (必須)

- 1.実装制限に起因するオペレーション問題の解決
- 2.IPsec の完全サポート

これについては、暗号化のための ESP、そして IKE、IKEv2 などの動的鍵交換プロトコルのサポートが求められます。

- 3.家庭内ノード管理機能のサポート

これについては、必要なプロトコル (UPnP、Rendezvous、Multicast DNS、など) を管理アプリケーションが実装する必要があります。

要求事項 (オプション)

IPv6 普及期のオプション的な要求事項としては、DNS の IPv6 トランスポート、新セキュリティ機構の実装 (SEND、DNSSEC) など、Mobile IPv6 の実装 (Client、Home Agent)、その他新しい仕様に対するサポートがあります。

PC (アプリケーション) の現状

有名なアプリケーションはデュアルスタック対応しつつあります。ただし問題も指摘されています。たとえば「IPv6 接続性がないネットワークで DNS の応答として AAAA が得られると、無条件に IPv6 接続を試みてしまう」というもので、これには OS が提供するライブラリに起因する問題と、独自の接続ロジックに起因する問題が関係しています。さらに、「IPv4 へのフォールバックが完全ではない、時間がかかる」「IPv6 アドレスが直接入力できない」といった点も指摘されています。

利用可能なアプリケーションの例としては、Web ブラウザ (HTTP クライアント)、FTP クライアント、電子メールクライアント、VoIP、SSH (リモートログイン)、インスタントメッセージが挙げられます。

アドレスファミリー独立の流儀に従っていないアプリケーションの存在も指摘されています。たとえば AF_INET、AF_INET6などをハードコードしている、RFC2553 形式のソケット API を使用していない (getaddrinfo()を使っていない) などです。

セキュリティ対策が十分ではないケースもあります。特に、各種ウィルスソフトの対策が不十分です。

PC (アプリケーション) の BCP

要求事項 (必須)

1.デュアルスタック化の促進

アドレスファミリー独立のプログラミング手法に対する啓蒙が必要です。プログラムの動作には関係しませんが、よりよいコードのためには重要なステップです。これについては、OS ベンダー、開発環境ベンダーが率先して行うべきです。ソケットレベル API はアプリケーションライブラリで隠蔽することも可能です。

また、フォールバック機構の導入も必要です。IPv4 のみの方が使いやすい、ということを減らすためです。OS の改修ができないのであれば、アプリケーション側で極力対応しなければなりません。適切なフォールバック機構の標準化が期待されます。

2.OS、アプリケーションの脆弱性が多く見つかった利用シーンでは、積極的な利用推奨は行

わない方がよい

セキュリティ上の責任を負わされかねないという問題が起こりかねないため、あえて推奨しない方がよいケースがあります。ただし、脆弱性がないアプリケーションにおいては、積極的に利用を推奨し普及を促進させるべきです。

3.統一されたユーザーインターフェース

IPv6 アドレスの入力方法など、アプリケーションが変わっても同じように扱えることが好ましいといえます。IPv4 の場合、“.”(ピリオド)を入力すると次のテキストボックスに移動しますが、IPv6 でもこれに相当する方法を導入すべきです。

また、ユーザーインターフェースを構成するIPv6 用語は標準的な用語を使用すべきです。IPv6 関連における推奨用語については、インターネット協会 IPv6 用語ワーキンググループが用語集を公開しています (<http://www.iajapan.org/ipv6/v6termwg.html>)。

要求事項 (オプション)

1.URL など FQDN を入力する欄における IPv6 アドレス (リテラル) のサポート

この機能は、問題の切り分け時に有効です。ただし、障害検出用アプリケーションのみの対応でもよいと考えられます。

2.補助機能に対する IPv6 サポート

Web ブラウザにおけるプロキシ自動設定スクリプト各種マクロ、スクリプト言語におけるサポート状況の改善など、アプリケーションごとの対応が望まれます。

プレイヤーにおけるシナリオ：ネットワーク機器提供者

ネットワーク機器提供者については、ネットワーク機器を以下に分類して検討します。

- ・レイヤ 1／レイヤ 2 機器
- ・レイヤ 3 以上機器 (複合機器含む)
- ・集合住宅用機器 (共用設置されるレイヤ 1 以上の機器)

複合機器は、レイヤ 3 以上の機器の組合せであるため、個別に扱いません。また、集合住宅用機器は要求機能が異なるため、単独で扱います。

レイヤ 1／レイヤ 2 機器の現状

スイッチングハブ、無線 LAN アクセスポイント、xDSL モデム、ケーブルモデム (ブリッジタイプ)、

メディアコンバータ、ONU などが対象となります。これらの機器は、基本的に IPv6 対応を意識しません。

ただし、上位レイヤ (レイヤ 3 以上) をチェックする無線 LAN アクセスポイントが存在します。この場合、独自認証処理が IPv4 前提で作られているなどから、IPv6 で通信できないケースが存在します。また、マルチキャストが通らない無線アクセスポイントが存在します。IPv6 マルチキャスト (MAC アドレス 33:33 で始まるもの) が通らないため、通信できない可能性があります。

レイヤ 1/レイヤ 2 機器の BCP

要求事項 (必須)

1. IPv6 の透過処理

IPv6 を透過できない機器について対応が必要です。これは基本的にハードウェアに依存するため、対応は困難です。解決策はリプレースのみとなります。EtherType を使ったフィルタ機能などでも IPv6 を確実にサポートする必要があります。

要求事項 (オプション)

[Multicast Traffic の局所化]

コンテンツ配信サービス視聴時に他の IP 電話やデータ通信が圧迫される事例があり、このため MLD Snooping 対応によるマルチキャストトラフィックの局所化が必要となります。しかし、コスト的に安価な機器への実装は困難です。

[QoS を確保したい]

絶対優先制御によって、IP 電話等リアルタイム性の高いアプリケーションの品質を保証するため、COS/TOS/TC/DSCP による優先制御への対応が求められます。しかし、安価な機器への実装はコスト的に困難です。

レイヤ 1/レイヤ 2 機器の IPv6 普及期

要求事項 (必須)

1. Multicast Traffic の局所化

MLD Snooping 対応によるマルチキャストトラフィックの局所化が可能となります。

2. QoS を確保

COS/TOS/TC/DSCP による優先制御対応を通じ、絶対優先制御で IP 電話などリアルタイム

性の高いアプリケーションの品質を保証するとともに、帯域保証で映像トラフィックなど一定の帯域を要求するアプリケーションの品質を保証することが必要です。

レイヤ 3 以上の機器 (複合機器含む) の現状

市販品ではハイエンドモデルのブロードバンドルータの一部が IPv6 対応済みで、デュアルスタックによる対応がなされています。しかし、普及モデルではコスト的な課題があります。ホスト型接続で使われる機器では IPv6 ブリッジ機能による対応が行われています。

事業者レンタルの場合、ルータ内蔵モデムの一部でデュアルスタック対応済みです。これは、現状で一般ユーザが最初に入手しやすい IPv6 対応ブロードバンドルータです。「サービスに加入したら、送られてきた機器が IPv6 に対応していた」といったイメージで導入されます。

IP 電話の IPv6 対応は進んでいません。これは、既存の IP 電話サービスが IPv4 を前提としているためです。閉じたネットワークでの IPv6 を使った TV 電話サービスはありますが、一般の IP 電話、加入電話、携帯電話との接続性は提供されていません。

レイヤ 3 以上の機器 (複合機器含む) の BCP

要求事項 (必須)

1.ブロードバンドルータにおける IPv6 対応

市販普及モデル (安価なモデル) での IPv6 対応が望まれます。

まず、IPv6 Ready Logo(Phase-1)相当の基本スタックの実装が求められます。

これに加え、サイト型接続では、現状の IPv6 サービスの有力方式である DHCPv6-PD の実装が必要です。PPPoE 接続の場合 IPv6CP が必要となります。

ホスト型接続の場合は、RA Proxy により、ブロードバンドルータでパケットをスルーせずにフィルタリング等の処理を行うことが求められます。

ファイアウォール機能の IPv6 対応も必須です。静的／動的パケットフィルタの実装が求められます。ICMPv6 フィルタ設定には注意が必要です (Path MTU Discovery 等の問題)。

この段階では、名前解決は IPv4 トランスポートで実現します。DNS Proxy 機能の AAAA レコード対応が求められます。DDNS 対応機器は、DDNS 登録時の AAAA レコード対応が求められます。

要求事項 (オプション)

[ブロードバンドルータにおける IPv6 対応]

以下の点で、ブロードバンドルータの IPv6 が望まれます。

- ・ IPsec (リモートアクセスおよび特定通信先との VPN 通信に利用)
- ・ Firewall Traversal (IPv4 の NAT Traversal 相当、UPnP が有力だが、標準化が待たれる)
- ・ セキュリティーのセキュリティ機能の IPv6 対応
- ・ IPv6 over IPv4 トンネルの実装 (DTCP、Configured、6to4、TSP、ISATAP、Teredo など。トンネル方式の統一が望まれる。サービス向けには認証機能付きの方式が望まれる)
- ・ IPv4/IPv6 トランスレータ機能の実装 (NAT-PT、SIIT 等。IPv4 端末で IPv6 サービスを享受したい場合、またはその逆のケース)
- ・ MLD Proxy (マルチキャストトラフィックの局所化が可能となる。マルチキャスト利用による低価格ライブ配信/VOD サービスの普及加速)
- ・ IPv4 で実現されている機能を徐々に IPv6 対応 (デュアルスタック化)
- ・ COS/TOS/TC/DSCP による優先制御対応 (絶対優先制御による IP 電話などリアルタイム性の高いアプリケーションの品質保証や、帯域保証による映像トラフィックなど一定の帯域を要求するアプリケーションの品質保証。事業者のサービスと連携した QoS ポリシーの設定)

レイヤ 3 以上の機器 (複合機器含む) の IPv6 普及期

要求事項 (必須)

1.VPN プロトコル (IPsec 等) の実装

リモートアクセスおよび特定通信先との VPN 通信に利用するため、必須となります。

2.Firewall Traversal (UPnP)

3.トランスポートの IPv6 対応

これは、DNS、UPnP にあてはまります。IPv6 しか使えない端末での通信に必要です。また、WWW 等の GUI、console/telnet 等の CLI でも IPv6 トランスポート対応が求められます。

4.セキュリティルータのセキュリティ機能の IPv6 対応

5.IP 電話の IPv6 対応

6.マルチホーミング

IPv6 では、サービスに応じた経路選択方式を採用する必要があります (ソースアドレスルーティング、レイヤ 4 以上ルーティングなど)。また、名前解決手段の検討が必要です (利用するサービスに応じた DNS サーバの選択など)。サービス提供形態に応じた始点アドレス選択方式を採用する必要あり (RFC3484 方式、サービスによって始点アドレスを決定、など)

7.MLD Proxy

8.COS/TOS/TC/DSCP による優先制御対応

絶対優先制御による IP 電話などリアルタイム性の高いアプリケーションの品質保証、帯域保証による映像トラフィックなど一定の帯域を要求するアプリケーションの品質保証、帯域制限、最低帯域保証などです。事業者のサービスや端末機器と連携した QoS ポリシーの設定 (UPnP QoS

の実装) が求められます。

要求事項 (オプション)

Trusted 3rd Party モデルの VPN 実装 (設定の簡略化, アクセスリストの一元管理が可能) と、Mobile IPv6 の Home Agent 機能実装が求められます。

集合住宅用機器の現状

メディアコンバータ、スイッチングハブ、VDSL コンセントレータ、Home PNA スイッチ、ONU など、レイヤ 1/レイヤ 2 機器であれば、基本的に IPv6 対応を意識しません。レイヤ 1/レイヤ 2 機器の項を参照してください。

レイヤ 3 機器では認証サーバ等の問題があります。レイヤ 3 以上機器に関する上記の説明をご覧ください。

集合住宅用機器の BCP

要求事項 (必須)

1. 認証サーバの IPv6 化

DHCPv6-PD、IPv6CP の認証サーバでのデュアルスタック対応が必須です。

2. レイヤ 2、レイヤ 3 機器によるユーザサイト分離 (セキュリティ SWG 参照)

IPv6 パケットフィルタリングによる RA、DHCPv6 等の分離が必要です。ホスト型の場合、同一リンク内にいる住民同士の通信のために上位ルータで以下のどちらかの対応が必要となります。

NDP Proxy

→家庭内端末同士の通信の場合、送信元端末は二者から NA を受信するが、RFC2461 に従った実装であれば Proxy 側からの NA の Override flag は 0(zero)であるため端末側からの NA の内容が優先

RAのon-linkをoff、ルータのICMPv6 Redirectをoff

→家庭内端末同士の通信がルータ経由

要求事項 (オプション)

[マルチキャストトラフィック配信:レイヤ 2 機器]

MLD Snooping への対応で、ユーザ (部屋) ごとにマルチキャストトラフィックが配信できます。

[QoS を確保したい: レイヤ 2、レイヤ 3 機器]

COS/TOS/TC/DSCP による優先制御対応で絶対優先制御による IP 電話などリアルタイム性の高いアプリケーションの品質保証、帯域保証による映像トラフィックなど一定の帯域を要求するアプリケーションの品質保証が可能になります。事業者のサービスと連携した QoS ポリシーの設定が望まれます。

集合住宅用機器の IPv6 普及期

要求事項 (必須)

1. 認証サーバでのリモートアクセス対応

認証サーバでリモートアクセスを終端する場合は、リモートアクセス通信を各ユーザ宅へ振り分ける機能が必要となります。また、ユーザ宅内でリモートアクセスを終端する場合は、認証サーバでリモートアクセスの通信を識別して認証する機能が必要です。

2. MLD Snooping 対応: L2 機器

この時期には、ユーザごとにマルチキャストトラフィックを配信できるようになる必要があります。

COS/TOS/TC/DSCP による優先制御対応: レイヤ 2、レイヤ 3 機器

IPv6 普及期には、絶対優先制御による IP 電話などリアルタイム性の高いアプリケーションの品質保証、帯域保証による映像トラフィックなど一定の帯域を要求するアプリケーションの品質保証、帯域制限、最低帯域保証が求められます。事業者のサービスと連携した QoS ポリシーの設定が必要です。

プレイヤーにおける移行シナリオ：通信ネットワーク提供者

通信ネットワーク提供者の移行シナリオについては、ISP SWG の移行シナリオを参照してください。

プレイヤーにおける移行シナリオ：サービス提供者

プレイヤーの分類では、サービス提供者を通信形態によって以下のように分類しました。

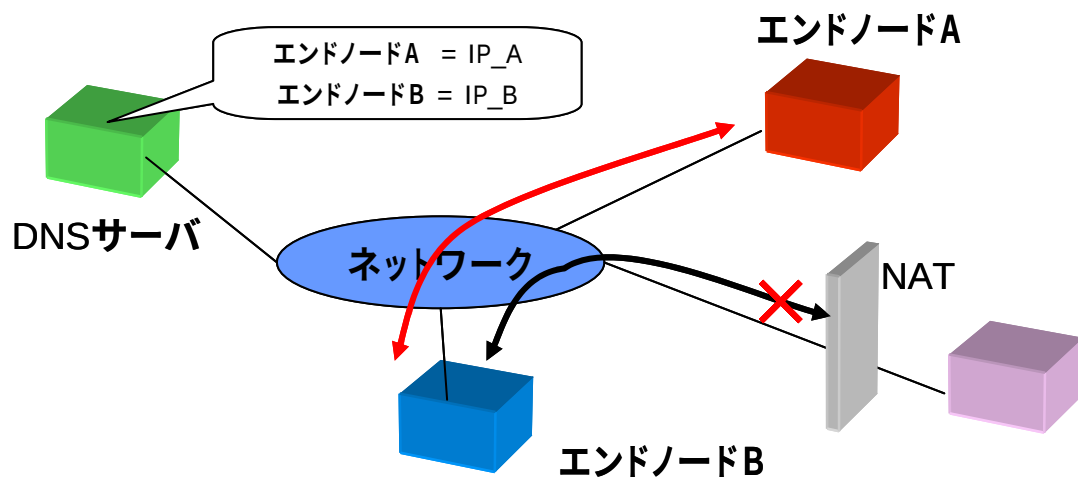
- (A) 完全 P2P 型
- (B) P2P+接続管理サーバ型
- (C) P2P+ロビーサーバ型
- (D) クライアント・サーバ型
- (E) クライアント・サーバ (ASP ポーリング) 型
- (F) クライアント・サーバ (クライアントポスト) 型
- (G) ホームサーバ型
- (H) 中央サーバ経由型

以下では、この分類にしたがって、各種サービス提供者の移行シナリオを検討します。

サービス (A) : 完全 P2P 型の現状

現状では、NAT の裏側にあるユーザは直接接続できず、P2P が利用しにくい原因となっています。このため、完全 P2P 型サービスでは、静的なポートフォワード、サーバ経由 (サービス (H) 型) など NAT を越える仕組みを使っています。

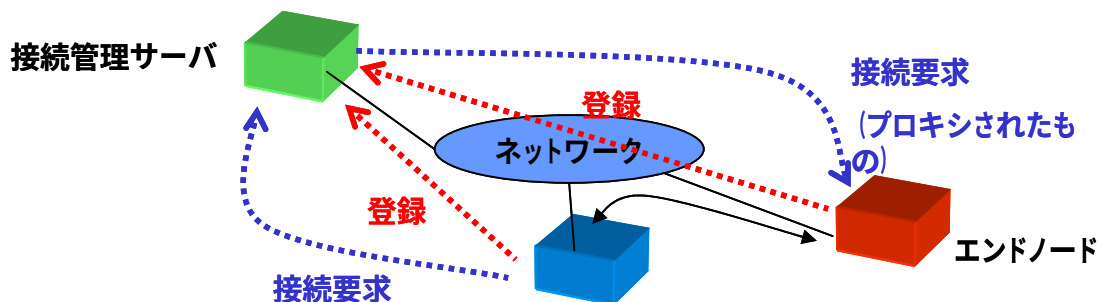
この場合、アクセス先となるアドレスは DNS などで公開されています。



サービス (B) : P2P+接続管理サーバ型の現状

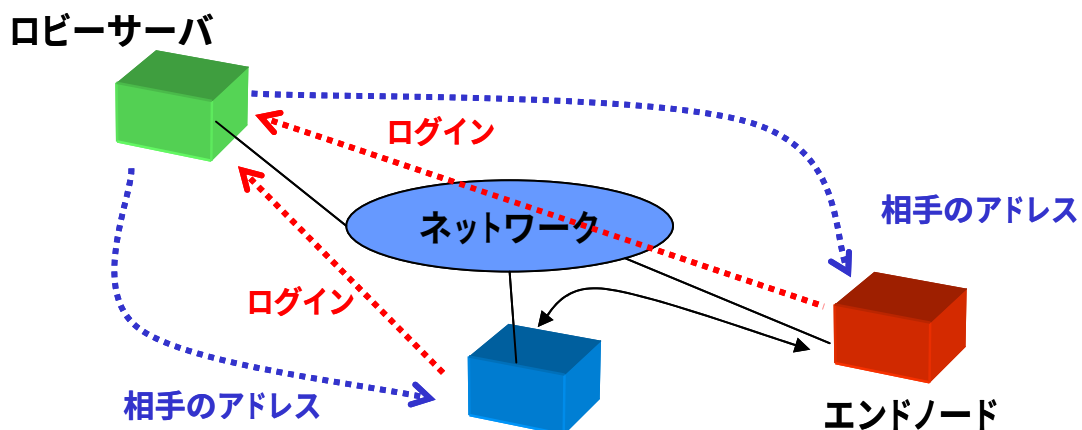
この種のサービスでは、通信相手を容易に発見する手段として接続管理サーバを利用しています。つまり、接続管理サーバは、ロビーサーバと接続可・不可の判断機能を提供しています。現状 (IPv4) に合わせたバックエンドシステム (ポリシー管理、会員管理、課金、サポートなど) が大規

模に構築されています。IPv4 サービスが中心ですが、VoIP では IPv6 を使ったサービスも登場しています。



サービス (C) : P2P+ロビーサーバ型の現状

このタイプのサービスでは、アプリケーション単位で通信相手を容易に発見する手段としてロビーサーバを利用しています。チャット、ストレージサービスなどの付加機能を提供する場合もあり、P2P 型ネットワークゲームで広く利用されています。NAT 問題は完全 P2P 型と同様に存在します。



サービス (D) : Client/Server 型の現状

現状では、これが最も利用されているネットワークサービスの形です。NAT の存在は (原則として) 通信に影響しません。

サーバソフトウェアの IPv6 化については、Web サーバ、Mail(SMTP)サーバ、FTP サーバ、

DNS サーバ、などの有名なソフトは対応済みです。

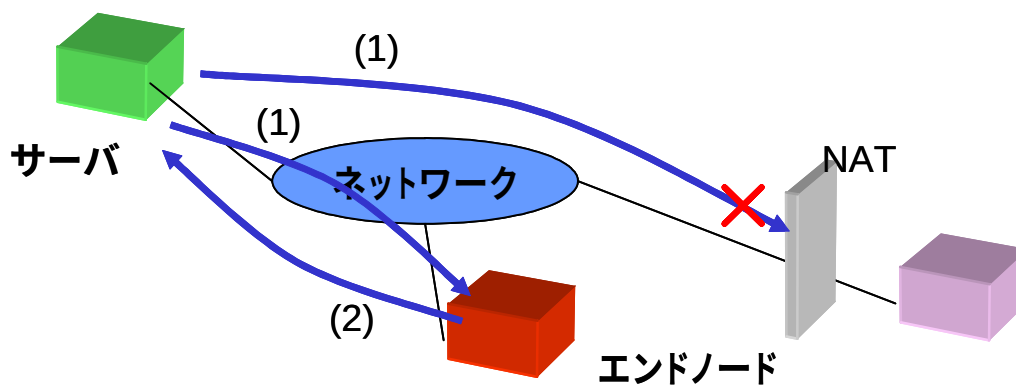
クライアントソフトウェアの IPv6 化については、Web ブラウザ、FTP クライアント、Mail (SMTP、POP、IMAP) クライアント、リモートアクセスなどの有名なソフトから対応が進んでいます。

インフラ側の対応待ちとなっているのは、クライアント側ネットワークの IPv6 接続性、DNS のレスポンス問題 (A と AAAA)、経路問題 (IPv4 経路と IPv6 経路の違い) です。

ソフトウェアの対応不足 (フォールバックが不十分、アクセスリストが正しく機能しないなど) も指摘されています。

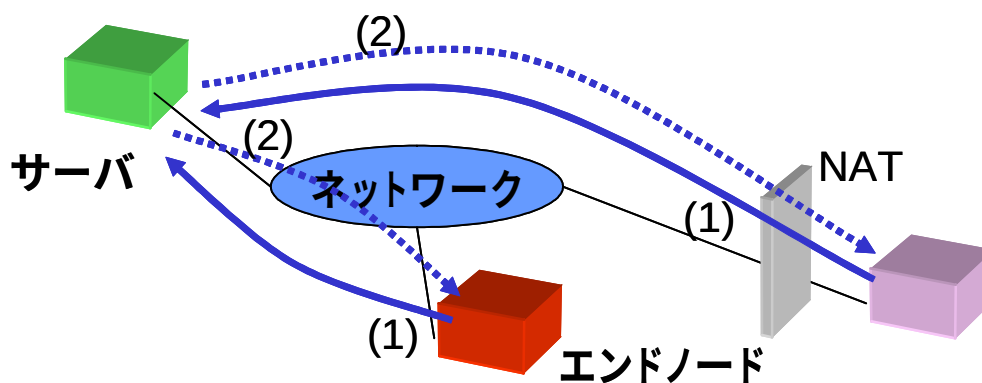
サービス (E) : Client/Server (ASP ポーリング) 型の現状

NAT が存在するため、ASP からポーリング対象ノードへの直接到達性が確保できず、ほとんど利用されていません。



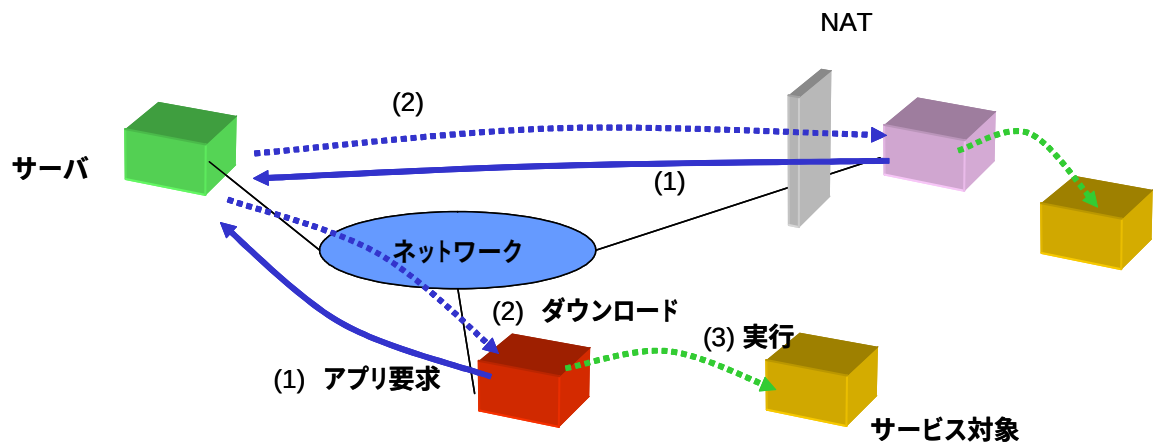
サービス (F) : Client/Server (クライアントポスト) 型の現状

このタイプのサービスは、ネットワークを利用するアプリケーションサービスの一部で利用されています。センサーからの情報送信や監視カメラからの情報送信に用いられているケースが見られます。NAT があっても、確実にデータを ASP に送信できるため、サーバポーリング型の代用として使われています。



サービス (G) : ホームサーバ型の現状

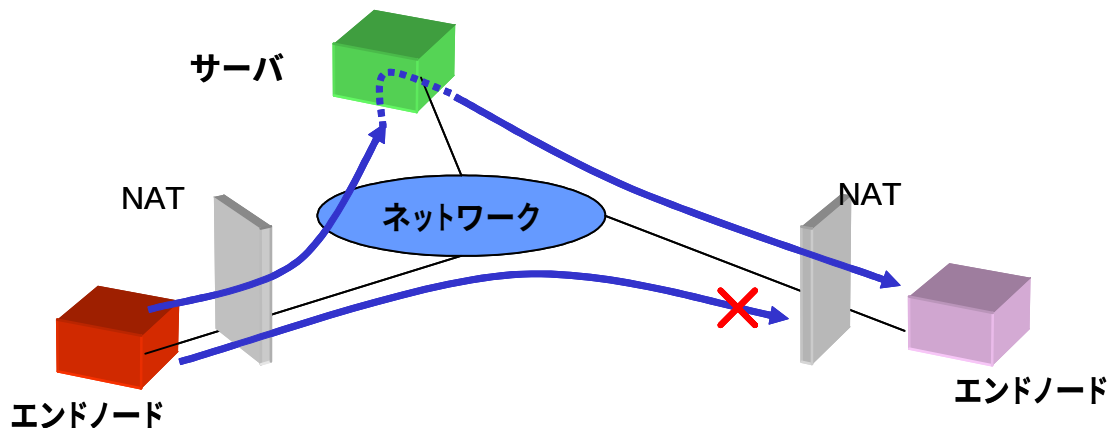
これは、通常の Client/Server 型 + 家庭内に閉じた通信の複合形態です。現状ではあまり利用されていません。アプリケーションプラットフォームに対する安全性を保证するため、ダウンロード元のアドレス以外とは通信できない場合がほとんどです。携帯電話用アプリケーションやファームウェアアップデートなどで、ダウンロードした先から他のノードと通信しない形態での利用は多いと考えられます。



サービス (H) : 中央サーバ経由型の現状

このタイプのサービスは、エンドノード間が直接通信できない場合に利用されています。

たとえば、VoIP などで、両方とも NAT の内側だった場合に最終的な代替手段として使われます。また、VPN サービスなど、プロトコル的に中央ノードが必須である場合があります。本来提供するサービスを支える目的で用いられていることが多いと言えます。



サービス共通の BCP

要求事項 (必須)

1. プロトコルのデュアルスタック対応

IPv6 対応を追加する際には、サービスで利用するプロトコルを再確認する必要があります。プロトコル中でアドレス情報を交換する場合には、IPv4/IPv6 の両方に対応するようにプロトコルを修正する必要があります。独自プロトコルを利用している場合には、細心の注意が必要です。

2. サーバソフトウェアのデュアルスタック対応

サーバの対応に関しては、フロントエンドで IPv6 通信ができるようにする、バックエンドで IPv6 情報をデータとして扱えるようにする、の 2 つが必要となります。

3. (クライアント) アプリケーションのデュアルスタック対応

IPv6、IPv4 の一方が使用できない場合に、適切に別の方法を試みるようにしておく必要があります。P2P 型通信を行うアプリケーションも同様です。また、サービスに関連するソフトウェアは、出荷後に更新できるようにすべきです。これは BCP 期であるため、IPv6 基本プロトコルの仕様変更が発生する可能性があるためです。バグフィックス対応、セキュリティ対応などのソフトウェア更新が必須です。対応が遅れたり、対応しなかったりすると製品の評価低下につながる恐れがあり、PL 法なども視野に入れた対応が必要です。

以降の BCP に関する記述では、各サービスのモデルごとに次の形式で分析します。

選択メリット

このモデルを選択することによってサービス提供者が得るメリットを列挙する

実現困難度： 1 (容易) ～5 (困難) の5段階評価

困難度の判定は以下の点を総合的に判断する

- ・技術的な困難さ (サービスに必要な技術が確立されていない場合は困難)
- ・IPv6 化 (移行、新規導入) に伴う必要作業量 (多い方が困難)
- ・サービス開始時の最低環境に対する外的要因の大きさ (多い方が困難)
- ・想定される収益元の大きさ (小さい方が困難)

要求事項

BCP 期にサービスを開始する際に必要な事項を整理する
(ネットワーク的な観点だけではなくサービス全体で列挙する)

問題点

BCP 期にサービスを開始する場合の問題点について

次ステップに進むためには

次のステップ (IPv6 普及期) に進むために改善すべき点について述べる

BCP 期の概要

この時期には、IPv6 ならではの機能を前面に押し出したサービスの急速な立ち上げは困難です。

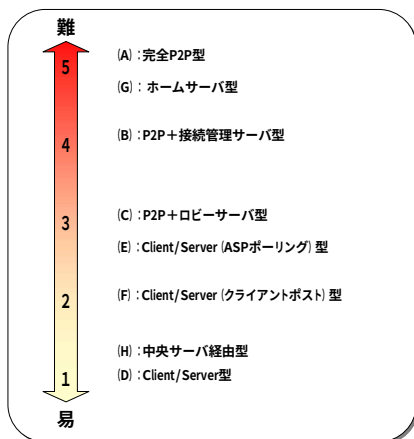
なぜなら、完全な P2P サービスの実現は、技術的な困難さ (安全な通信、名前解決など) を伴いますし、サービスとしてのビジネスモデルが見出せていません。ホームサーバ型サービスの実現には、汎用的なプラットフォームの不在が課題となります。マルチキャストは、利用できるアクセス網が限定されるほか、ユニキャストトンネルの併用を避けることができません。さらに、ソフトウェアとハードウェアを一括して提供できる場合は Client/Server (ASP ポーリング型) サービスなど、別のアプローチが可能です。

IPv4 で提供されている既存サービスのデュアルスタック化は容易に実現できます。Client/Server 型、中央サーバ経由型、Client/Server (クライアントポスト) 型はすべてあてはまります。

3.2.4. プレイヤーにおける移行シナリオ (サービス提供者編)



■ BCP期 概要



■ IPv6ならではの機能を前面に押し出したサービスの急速な立ち上げは困難

- 完全なP2Pサービス
 - 技術的な困難さ (安全な通信、名前解決など)
 - サービスとしてのビジネスモデルが不在
- ホームサーバ型サービス
 - 汎用プラットフォーム不在
- マルチキャスト
 - ネットワークが限定される
 - アクセス網限定
 - ユニキャストトンネルの併用
- ソフトウェアとハードウェアを一括して提供できる場合は別のアプローチが可能
 - Client/Server (ASPポーリング型) サービス

■ IPv4で提供されている既存サービスのデュアルスタック化は容易に実現できる

- Client/Server型
- 中央サーバ経由型
- Client/Server (クライアントポスト) 型

Oct 8, 2004

IPv6PC Transition WG Home SWG

176

サービス (A) : 完全 P2P 型の BCP

選択メリット

この方式の選択メリットは、第三者に影響されない通信が実現できることにあります。第三者によらない信頼性の確保と、エンドツーエンド通信による低遅延の実現が可能です。

実現困難度: 5

○ソフトウェアの開発困難度は低いです

×ネットワーク関連の技術的問題が多数存在します。具体的には、名前解決 (問い合わせと登録)、ファイアウォールとの連携、アクセス制御、(既存サービスがある場合) IPv4 ユーザとの共存、などです。

×上記の技術的問題、インターネットへの IPv6 アクセスなど、このサービスの実現に必要な外的要因は多数あります。

○サービスとしてのビジネスモデルが確立していない現状では、ソフトウェア販売と若干のサポートに頼らざるを得ません。しかし、ディプロイメントの影響範囲が狭く、ビジネス以外では実現しやすい方式と言えます。

要求事項

要求事項としては、ダイナミック DNS サーバの運用があります。

問題点

DNS を使って IP アドレスを公開せざるを得ず、プライバシーなどの問題に発展する可能性があります。また、ソフトウェアの売り切りになってしまい収入源が乏しいという問題があります。

次ステップに進むためには

ダイナミック DNS などの公開名前解決技術とプライバシーの両立、P2P 通信の安全性確保 (汎用的な暗号化方式の採用、容易なアクセス制限) など、技術的課題の解決が求められます。

また、ソフト販売以外の収入源の確保が必要です。サービス利用に必要なハード、ソフト、サポートをセットにして収入を上げるビジネスモデルが考えられます。

サービス (B) : P2P + 接続管理サーバ型の BCP

選択メリット

この方式の選択メリットとしては、

- ・接続管理サーバで通信相手を決定するために名前解決に関する問題を解消できる
- ・接続管理サーバが通信制御や暗号鍵交換の仲介をすることで安全性が向上する
- ・接続管理サーバを通して継続的な会費収入が望める

が挙げられます。

実現困難度: 4

○この方式では管理サーバを介するので安全性が向上します。Trusted 3rd Party Model と組み合わせることでさらに安全性が向上します。

○この方式による P2P ソフト開発の困難度は低いといえます。

× (既存サービスがある場合) IPv6 と IPv4 との共存に難があります。

× 接続管理サーバとバックエンドサーバ (データ) の IPv6 対応が必要です。

× (IPv6 環境下における) 管理サーバの運用、接続ポリシーの管理・適用ノウハウを積む必要があります。

△ファイアウォールとの連携を除けば、技術的問題は比較的少ないといえます。

△必要な外的要因は、上記の技術的問題、インターネットへの IPv6 アクセスなどやや多いといえます。

○会員への接続管理サーバ提供による継続的収入が望めます。

要求事項

要求事項は IPv6 に対応した接続管理サーバを運用する必要があることと、サービスに利用する内部データ形式を IPv6 に対応する必要があることです。

問題点

すでに IPv4 でサービスを提供している場合、IPv4 環境を利用しているユーザとの共存が問題となります。アプリケーション、サーバをデュアルスタックに対応させたとしても、IPv4 NAT ユーザとの通信は困難です。

また、接続管理サーバ、バックエンドサーバが Single Point of Failure になるため、運用コストが高いといえます。

次ステップに進むためには

次ステップに向けては、以下が求められます。

- ・IPv4 との親和性強化 (サービス (H) の形態を利用してトランスレータ機能の提供、など)
- ・通信の安全性確保 (P2P 通信部分、接続管理サーバとの通信部分)
- ・P2P 通信部分の品質向上 (バックボーン、アクセスなどネットワーク全体の品質向上、QoS など)
- ・オールインワンパック (アクセス回線の IPv6 化、ハードウェア、ソフトウェア、サポート) などの導入による大規模導入

サービス (C) : P2P + ロビーサーバ型の BCP

選択メリット

この方式では、ロビーサーバで通信相手を決定するため、名前解決に関する問題を解消できます。利用者側も P2P 通信を強く意識する必要がありません。

また、対向ノードの IPv6 アドレスがロビーサーバから通知されるため、将来的にファイアウォール制御などにも応用できる可能性があります。

さらに、ロビーサーバを通して継続的な会費収入が望めます。

実現困難度: 3

- P2P ソフト開発の困難度は低いといえます。
- × (既存サービスがある場合) IPv4 との共存に難があります。
- ×ロビーサーバ、バックエンドサーバ (データ) の IPv6 対応が必要です。
- ファイアウォールとの連携以外、技術的問題は比較的少ないといえます。
- △上記の技術的問題、インターネットへの IPv6 アクセスなど必要な外的要因はやや多くあります。
- 会員へのロビーサーバ提供による継続的収入が望めます。

要求事項

この方式では、IPv6 に対応したロビーサーバを運用する必要があり、サービスに利用する内部データ形式を IPv6 に対応する必要があります。

問題点

(すでに IPv4 でサービスを提供している場合) IPv4 環境を利用しているユーザとの共存が問題となります。アプリケーション、サーバをデュアルスタックに対応させても IPv4 NAT ユーザとの通信は困難です。

また、ロビーサーバが Single Point of Failure になるため、運用コストが高くなりやすくなります。

次ステップに進むためには

次ステップに向けては、

- ・IPv4 との親和性強化 (サービス (H) の形態を利用してトランスレータ機能の提供、など)
- ・ロビーサーバでの付加機能による集客力向上
- ・通信の安全性確保 (P2P 通信部分、ロビーサーバとの通信部分)
- ・P2P 通信部分の品質向上 (バックボーン、アクセスなどネットワーク全体の品質向上、QoS など)
- ・オールインワンパック (アクセス回線の IPv6 化、ハードウェア、ソフトウェア、サポート) などの導入による大規模導入

が求められます。

サービス (D) : Client/Server 型の BCP

選択メリット

この方式では既存サービスをほとんど変更することなく IPv6 を導入できます。

実現困難度: 1

○技術的な問題はほとんどありません。IPv4 と同じ通信形態なので、IPv4 と同じ技術がそのまま利用できます。

○オープンソース系サーバソフトの IPv6 化はほとんど完了しています。ただし、独自サーバを使用している場合には、対応が必要です。

○インフラ (データセンタなど) の整備も進んでいます。

※データセンターのセクションも参照してください。

[注意]

この形態では IPv6 化に伴うコストを直接回収することができません。

- ▶ 現状 (IPv4) でおなじことが実現できているためです。
- ▶ IPv6 化のコストを回収するためには独自に IPv6 のメリットを活用するサービスを導入する必要があります。たとえば、サービス (B)、サービス (E) の併用などが考えられます。本形態はそのための移行ステップであると捕らえることができます。
- ▶ NAT Traversal が不要になるなど比較的小さなメリットはありますが、移行コス

要求事項

IPv6 に対応したフロントエンドサーバを運用する必要があり、サービスに利用する内部データ形式を IPv6 に対応する必要があります。

問題点

課題としては、運用者の教育、ログ管理があります。また、大規模なバックエンド、データベースの移行が必要となり、特に実運用しているデータを移行する際は細心の注意が必要です。

次ステップに進むためには

次ステップに向けては、サーバの信頼性向上、ログ管理手法の確立に加え、IPv6 のメリットを直接的に活用するサービスの検討、導入が求められます。

サービス (E) : Client/Server (ASP ポーリング) 型の BCP

選択メリット

既存 (バックエンド) サーバ設備が流用でき、初期コストを抑えることができます。この方式では、ASP 側から情報を任意のタイミングで提供することができるほか、ASP からポーリングするため利用するネットワーク帯域を把握することができます。

実現困難度: 2～4

△技術的な問題はやや多いといえます。このモデルは小型組み込み機器の登場が予想されるため、小型組込機器特有の問題が発生します。たとえばポーリングのタイミングとファイアウォールの連携などです。

△C/S 型既存サービスから移行する場合にはバックエンドサーバ、データの移行が必要です。

△ポーリングに対応する専用機器 (またはソフト) をユーザ側に設置する必要があります。この際、ソフト、ハードを一括して提供できる場合はメリットになりえます。ソフトのみ、付加サービスのみを提供する形態は、BCP では困難です。

○ユーザの知らないうちに IPv6 を利用してしまうようにすることが可能です。たとえば、テレメータリングなど、アクセス回線や機器を含めたトータルソリューションとして展開できます。

要求事項

IPv6 移行では、IPv6 でのポーリングに対応した機器、ソフトウェアの提供や、ASP の安定運用 (収集データの管理など) が要求されます。また、既存サービスから移行する場合、バックエンドサーバの移行が必要です。

問題点

まず、ポーリング間隔とサービスクオリティのバランスが問題となります。間隔を狭くすると、より多くの帯域が必要となります。

また、家庭内に設置された機器に対する到達性の確保、特にファイアウォールとの連携が課題となります。

次ステップに進むためには

次ステップに向けては、ポーリングによるデータ収集ノウハウの蓄積 (ポーリング間隔と帯域の管理) や、ポーリングされる側のノードの小型化、省電力化、低価格化が求められます。また、安全な通信路の確保が課題となります。

サービス (F) : Client/Server (クライアントポスト) 型の BCP

選択メリット

このタイプのサービスでは、既存サービスをほとんど変更することなく IPv6 を導入できます。初動が顧客側にあるため、IPv4 ノードと IPv6 ノードの共存も容易です。将来的に IPv6 ユーザが増加すれば ASP ポーリング型に移行することも可能で、そうすれば ASP ポーリング型のメリットも享受できることになります。

実現困難度: 2

○技術的な問題はわずかです。IPv4 と同じ通信形態なので、IPv4 と同じ技術がそのまま利用できます。ただし、このモデルは小型組み込み機器の登場が予想されるため、小型組み込み機器特有の問題が発生します。

△C/S 型既存サービスから移行する場合にはバックエンドサーバ、データの移行が必要です。

○ユーザの知らないうちに IPv6 を利用してしまうようにすることが可能ですし、機器をデュアルスタックにしておけば、IPv4 でも同様にサービスを提供することができます。さらに、ホームネットワークが IPv6 で接続された後にポーリング型に切り替えることができます。

○『IPv4 ポスト型→IPv6 ポスト型→IPv6 ポーリング型』というような移行シナリオが描けます。

要求事項

要求されるのは、IPv6 で情報をポストする機能を持った機器、ソフトウェアの提供、ASP の安定運用、そして既存サービスから移行する場合にはバックエンドサーバの移行です。

問題点

クライアントに設定するポスト間隔とサービスクオリティのバランスをどう取るかという問題があります。間隔を狭くしすぎると大きな帯域を消費します。

イベントドリブンだと(ノード数の増加により) DoS が自然発生する可能性も否定できません。また、イベントドリブンの場合には、トラフィックパターンが推測される可能性があります。

次ステップに進むためには

次ステップに向けては、多量のノードを使ったデータ収集ノウハウの蓄積、クライアントがポストするデータ間隔の制御と ASP 側の帯域管理、データをポストするノードの小型化、省電力化、低価格化、そして安全な通信路の確保が求められます。

サービス (G) :ホームサーバ型の BCP

選択メリット

この方式では、アプリケーションダウンロード部分は C/S 型サービスとなるメリットがあり、月額料金制などを導入することで継続的な収入が見込めます。また、携帯電話用アプリケーションなど利用者にとって馴染みのある形態です。

実現困難度: 5

×家庭内で複数のノードを連携させるためのインタフェース、プロトコルが確立していません。

×ダウンロードしたアプリケーションが他のノードと通信する際の安全性を保証する方法が確立していません。

要求事項

ホームサーバなどの実行プラットフォーム、家庭内ノードを制御するためのインタフェースなど、アプリケーションプラットフォームの確立が求められます。ダウンロードされるアプリケーションを提供する必要があります。

問題点

問題としては、

- ・ アプリケーションの安全性をいかにして保証するかという点があります。具体的には、アプリケーションの安全をどのように保証するか、また、安全が保証されたアプリケーションからのアクセスであることを、アクセスされる側のノードが確認する手段はあるのかという点です。
 - ・ アプリケーションプラットフォーム／ソフトウェアの数が少ないとビジネスにならないという問題もあります。仕様の共通化が必要（例：携帯電話アプリケーション）ですが、クローズドプラットフォームでもよいのであれば、サービスは開始できます。
- といった点が指摘できます。

次ステップに進むためには

次ステップに向けては、安全な実行環境の提供が求められます。このためには、ダウンロードした先で IP/IPv6 以外の方法で通信する（たとえば赤外線？）という方法もあります。

また、アプリケーションプラットフォームの共通仕様の確立が求められます。

サービス (H)：中央サーバ経由型の BCP

選択メリット

このタイプの選択メリットは、次の通りです。

- ・各通信が単純な C/S 型になるため、既存技術が流用できる
- ・サーバで通信制御などを提供することで安全性が向上する
- ・信頼できるサーバが暗号鍵交換の仲介をすることで安全性が向上する
- ・サーバがトランスレータ機能を実行することで、IPv4 ノードと IPv6 ノードの相互通信が実現できる
- ・中央サーバが通信相手を隠蔽するので高いプライバシー保護が可能
- ・中央サーバを必ず介するので課金サービス等に利用できる

実現困難度： 1～2

○技術的な問題はわずかです。IPv4 と同じ通信形態なので、IPv4 と同じ技術がそのまま利用できますし、トランスレータはアプリケーションレベルで中継することで確実な中継が可能です。

△既存サービスから移行する場合にはバックエンドサーバ、データの移行が必要です。

○IPv4 との共存が容易に実現できます。

○サーバ利用料により継続した収入を確保できます。

要求事項

加入者からの接続を処理するフロントエンド部分、IPv4 を利用する加入者と IPv6 を利用する加入者を相互接続するトランスレータ部分など、中継サーバの IPv6 対応が求められます。

また、バックエンドサーバが IPv6 情報をデータとして扱えるようにする必要があります。

問題点

問題点としては、ユーザ数が増加すると、トラフィック量、サーバ負荷が激増することと、サーバが Single Point of Failure になることが挙げられます。

次ステップに進むためには

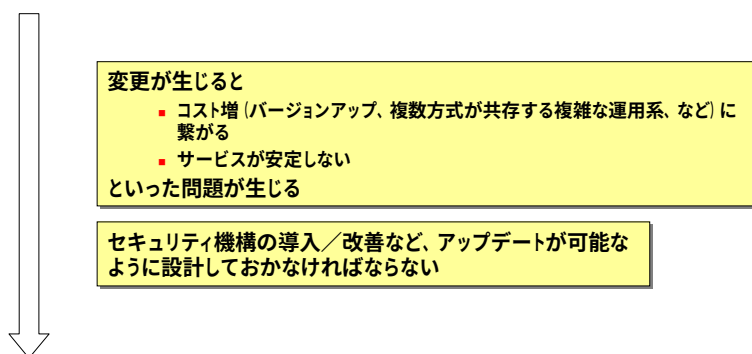
次ステップに向けては、安全な中継サーバの運用方式の確立（加入者が共に信頼するサーバを提供）が求められます。また、トラフィック集中を回避する運用ノウハウの蓄積が求められます。

以上がサービス形態別の BCP です。サービス提供者に関して一般的に指摘できるのは、いったん BCP 期に達してしまえば、そのサービス内容は、IPv6 普及期に提供されるものとあまり差異がないということです。逆に、差異が大きいようではコストが増大しますし、サービスも不安定になります。したがって、BCP 期に十分な検証を行い、ノウハウを蓄積しておく必要があります。

3.2.4. プレイヤーにおける移行シナリオ（サービス提供者編）



サービス提供者のIPv6普及期（移行完了期）は、BCP段階と差異は少ないと考えられる



BCP期に十分にシミュレーション、試験、トライアル（ベータサービス）を重ねておくことが重要

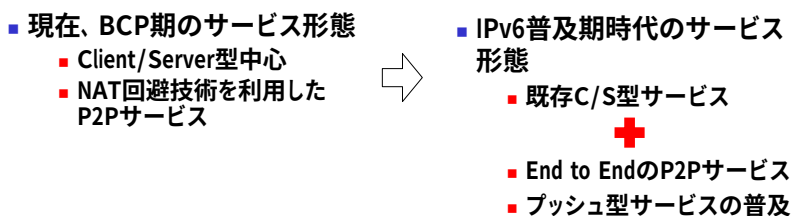
サービスの形態変化に関しては、次のことが指摘できます。

現在、そして BCP 期には既存の C/S 型サービス、そして各種の NAT 回避テクニックを利用した P2P サービスが主流です。しかし、IPv6 普及期にはエンドツーエンド型の P2P サービスやプッシュ型サービスが普及するようになってきます。

こうした新形態のサービスを IPv6 とともに広めていく時期の注意点としては、新形態での運用ノウハウの蓄積に加え、膨大な数の端末に対するサービスが十分に提供できる体制作りが求められます。

また、こうした新形態のサービスでは IPv4 端末について、サポートするかどうか、ユーザーサポートをどう提供するか、といった点をあらかじめ十分に検討していく必要があります。

3.2.4. プレイヤーにおける移行シナリオ (サービス提供者編)



新形態サービスの台頭

- 新しいサービス形態に対する
 - 膨大なノードに対するサービスが提供可能なシステムづくり
 - 運用ノウハウの蓄積が重要
- IPv4ノードに対する対処方法を明確に決めておくことが望ましい
 - サポートするか、否か、その期間は、など
 - 障害発生時、ユーザサポート時、など

IPv6 普及期時代のサービス提供者に対する要求

IPv6 普及期時代はセンサーの用途拡大など、『サービスの横展開が期待される』と考えられています。

たとえば、BCP では専用 ASP としか通信しなかった防犯センサーが、IPv6 普及期では PC や家庭内コントローラなどの汎用品にもデータを送るようになります。この結果、家庭内の集中モニタリングが可能になります。

さらに、BCP ではセキュリティを提供する ASP としか通信しなかったセンサーが、(ユーザの意図によって) ホームヘルスケアを提供する ASP にもデータを提供するようになる、といった発展が考えられます。

したがって、次のような技術的要求が生まれます。

- ・サービス (アプリケーション) プロトコルの標準化
- ・サービス (アプリケーション) プロトコルの相互変換技術の確立
- ・家庭内におけるサービス発見や名前付け (ネーミングの項を参照) の手法の確立 (厳密にはサービス提供者が実施するものではない)
- ・個人情報保護のため、収集した情報の保護の徹底

IPv6 普及期時代はこれまで以上に『通信内容が個人、利用者の生活に密接に関連』する時代です。

センサーによる情報収集が広がり、IPv6 アドレスによるエンドノード特定を生かせる可能性が出てきます。そしてこうした情報を連携させることで、より有意なサービスが提供できるようになります。そのためには、前記のサービスの横展開とも関連しますが、相互接続が可能な認証、暗号化機構の採用が求められます。この点では、安全かつ容易な手法が期待されています。

技術的要求としては、ユーザスキルを要求しない容易な暗号、認証機構を採用しなければなりません。情報を確実に守る暗号化機構、そして情報利用者を限定できる認証機構が必要です。社会的要求にも応えなければなりません。

BCP→IPv6 普及期の移行期におけるサービス提供者のネットワークインフラに対する影響

C/SからP2Pへの移行

これにより、サービス提供者 (ASP) に流れるトラフィックが減少します。ただし、ロビーサーバ、接続管理サーバが付加機能を提供すると (チャット、掲示板など) 減少しない可能性があります。これは、付加機能が C/S 型になるためです。

また、移行期にサーバが IPv4/IPv6 変換機能を提供する場合、サーバを経由するトラフィックが激増する可能性があります。特に BCP→IPv6 普及期の移行初期 (一般ユーザにサービスが認知された後) に注意が必要です。

そして、ユーザ間トラフィックの増加に伴い、バックボーンのトラフィックパターンが変化します。

IPv6 を利用する小型組込ノードの普及

クライアントポスト型サービスを行う場合、流入トラフィック量、頻度、規則性を正しく把握することが重要になります。このタイプのサービスでは、ノードの接続要求を制御できないため、ASP ポーリング型サービスよりも問題が深刻化しやすいという問題があります。

バックエンドサーバ (DB、管理系) に関しては現状の IPv4 ノウハウを使って増強等を行えばよいと考えられます。

4. IPv6 普及期に向けての課題

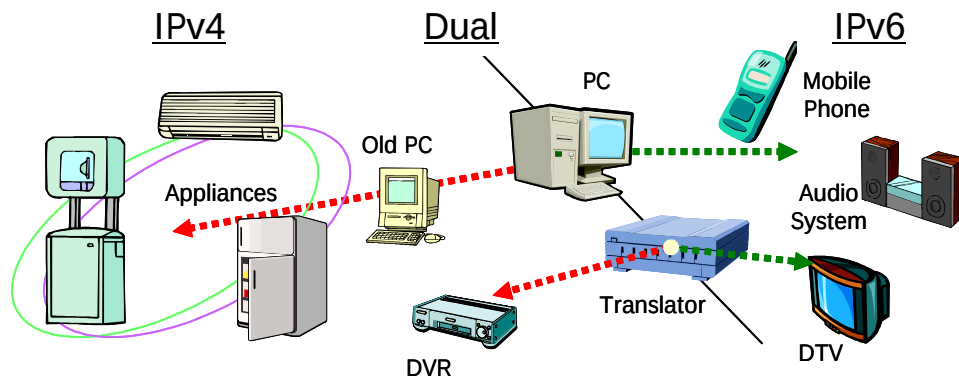
IPv6 普及期に向けての課題

トランスレータ機能

トランスレータ機能とは、IPv6 と IPv4 の変換を実現する技術のことで、NAT-PT、ALG、TCP Relay などが挙げられます。NAT-PT については『IPv6 Ready Logo Program Phase-2』が用意される予定です。

トランスレータのメリットは、IPv6 のみの機器と IPv4 のみの機器を連携させる必要性に依存します。特に、家庭へのトランスレータの導入は各家庭の状態に依存します。IPv4 機器が多い場合、トランスレータは有用ですが、IPv4 機器が少ないならば、トランスレータの効果が少ないといえます。

しかし、ベンダーが既存製品との相互通信を保証したい場合など、明確な利用目的がある場合は導入するべきです。

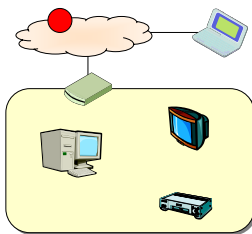


トランスレータ機能を設置する位置は、アプリケーションに依存します。

下図に、家庭外にある場合、ルータ上にある場合、PC 上にある場合の 3 つに分けて、メリットとデメリットを示します。

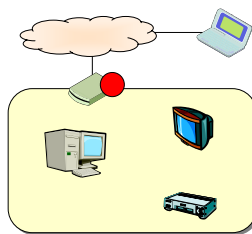
4.1.1. トランスレータ機能

■ 設置位置: アプリに依存



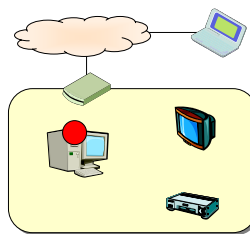
家庭外にある場合

- 遠隔アクセスサービスの一環として提供
[メリット]
- 家庭内には複雑な設定が不要
[デメリット]
- 家庭内ではIPv4⇄IPv6の変換ができない
- 家庭内のIPv4ノードにアクセスするためには使用できない



ルータ上にある場合

- ブロードバンドルータの一つの機能として提供
[メリット]
- IPv4⇄IPv6双方向の変換が可能
(ルータがグローバルIPv4アドレスを持つ場合のみ)
[デメリット]
- ルータの設定が複雑化
- 設定ミスによるセキュリティ低下



PC上にある場合

- PC上の一つのソフトとして提供
[メリット]
- PCアプリなので導入が容易
[デメリット]
- PCの設定が複雑に (パーソナルファイアウォールなども関連)
- 他の機器からは使いにくい

ネーミング

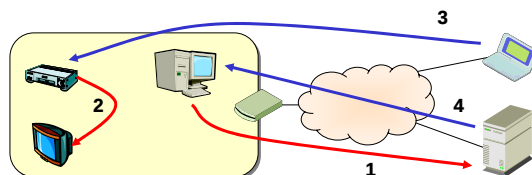
ネーミングとは、機能的には、登録/解決、DNS サーバ発見、名前付け方法を総称する言葉です。方法的には、クエリの送信方法、DNS サーバの発見方法、トランスポートプロトコルが必要です。名前解決の目的によって、下のように分類されます。

4.1.2. 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

Oct 8, 2004

IPv6PC Transition WG Home SWG

202

家庭内での名前解決の課題

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ります。

DNSサーバ発見プロセス

これについては、Multicast か Anycast か、さらに自動設定プロトコルを使うか手動設定なのか、サーバ不要方式を使うのかといった判断が求められます。

機器情報の登録

機器の名前登録について、DNS の枠組みを使うのか、DNS 以外の枠組みを使うのか、IP アドレス、その他の付加情報をどう登録するかといった検討が必要です。

クエリモデル

問い合わせの形態としては、Multicast、Anycast、Unicast、ICMPv6 Node Information Query といった選択肢を検討しなければなりません。

ドメイン名

ドメイン名については、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 から委譲されるべきか、利用者が適当に命名すべきか、といった点を考えなければなりません。

家庭内の名前解決への対応案

上の検討課題への対応案は以下の通りです。

DNSサーバ発見プロセス

設定するインタフェースを持たない機器が存在することから、自動設定の必要性があります。

well known Anycast、Multicast の使用により設定を省略することが可能ですが、セキュリティに関する検討が必要です。

IETF による議論(draft-ietf-dnsop-ipv6-dns-configuration)では、RA、DHCP、well known multicast の3方式が列挙されており、1つには絞りとまかれていません。このドラフトには、各方法に対する利点と欠点が整理されています。

また、non-PC 主導による IPv6 の普及シナリオが描けた場合、DNS サーバに依存しない別の方法が登場する可能性もあります。

クエリモデル

Unicast は、既存 DNS の通りです。

Anycast では、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です。Anycast アドレスは DHCP で配布してもよいですし、Well Known のアドレスを定義することも可能です(現状未定義)。

Multicast では、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ほか、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です。これは、Multicast DNS の場合には、問い合わせは転送されないためです。

ICMPv6 Node Information Query は DNS ではありません。このため、プログラムの修正が必要となります。まず、問い合わせ側ではレゾルバを改造し、OS 上は通常の名前解決機構として利用できるようにしなければなりません。応答側も Node Information Query に対する対応が必要となります。

Anycast、Multicast DNS に関しては、セキュリティの問題があります。つまり、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証がないという点です。

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です。それは、表示装置、入力装置を持たない機器が存在するからです。また、IPv6 普及期の世界では多数のノードが接続する可能性があることから、自動登録手段は必要です。したがって、DNS UPDATE など、接続検出(アドレスの変更)と自動登録の連携が求められます。

物理的な位置との対応関係については、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くなります。DNS 上に登録する情報は『camera01』で

もいいですが、ユーザに見せるためには変換が必要となります。

機器の登録に関する問題点としては、どの範囲に公開するのか、つまりプライバシーの扱いをどうするかという点、さらに名前の付け方として、同一機種が複数存在する場合どう区別するのかという点があります。

家庭外からの名前解決の課題

これまでは家庭内での名前解決についてでしたが、家庭外ノードが家庭内ノードを解決したい場合（つまり先ほどの分類ではケース3と4）における課題としては、以下のような登録に関する点があります。

- ・DDNS、DNS updateなどをどのように使うか
- ・登録先は ISP 提供サーバ、機器ベンダー提供サーバ、第三者提供サーバといった選択肢がある
- ・登録情報、登録対象機器を決定する必要がある
- ・情報の公開先、公開内容を定める必要がある
- ・プライバシーを確保しなければならない

家庭外からの名前解決の対応策

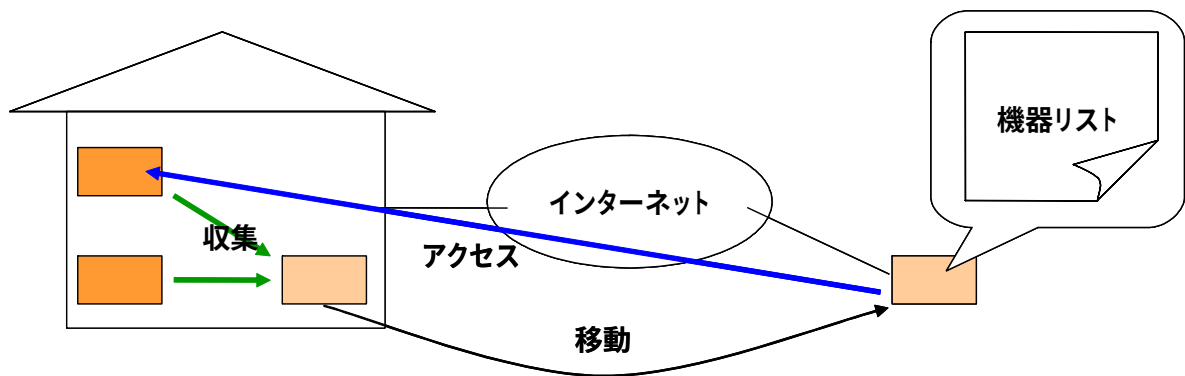
対応策の前提として、一般の家庭で（外部公開用）DNS サーバを運用することは不可能だといふことがあります。

ドメイン名の委譲問題もありますし、もともと家庭で DNS サーバは管理できません。ただし、DNS クエリの中継や、内部用簡易 DNS サーバの利用は行われます。

したがって、解決の基本的な方針としては、家庭外のノード内で解決する、インターネット上に情報が存在する、の 2 通りのうちのいずれかということになります。具体的には、以下のようなモデルが考えられます。

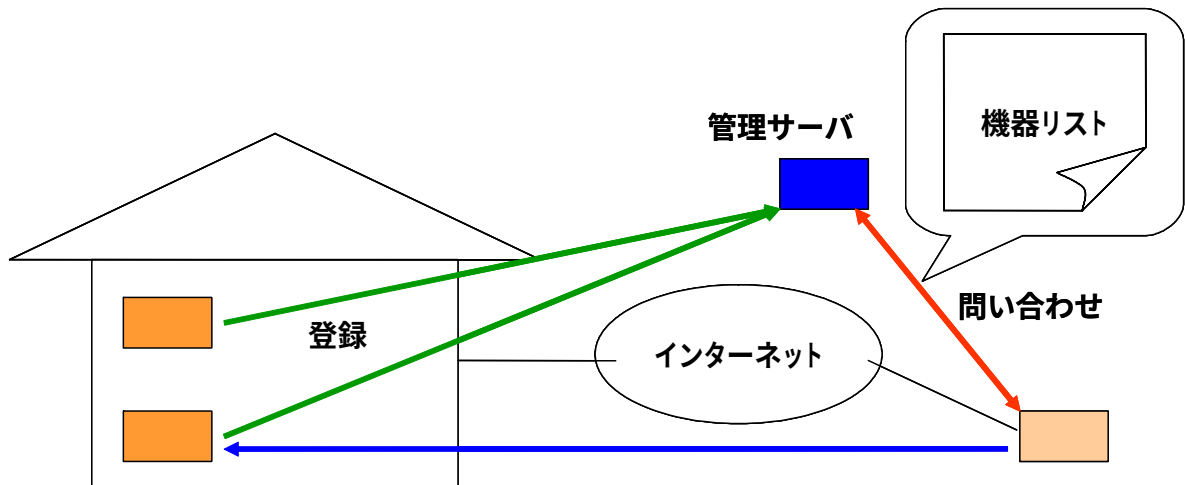
事前収集モデル

たとえば各端末が/etc/hosts を持つことが考えられます。この場合、情報はノードの内部にのみ存在するので安全ですが、ノード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。



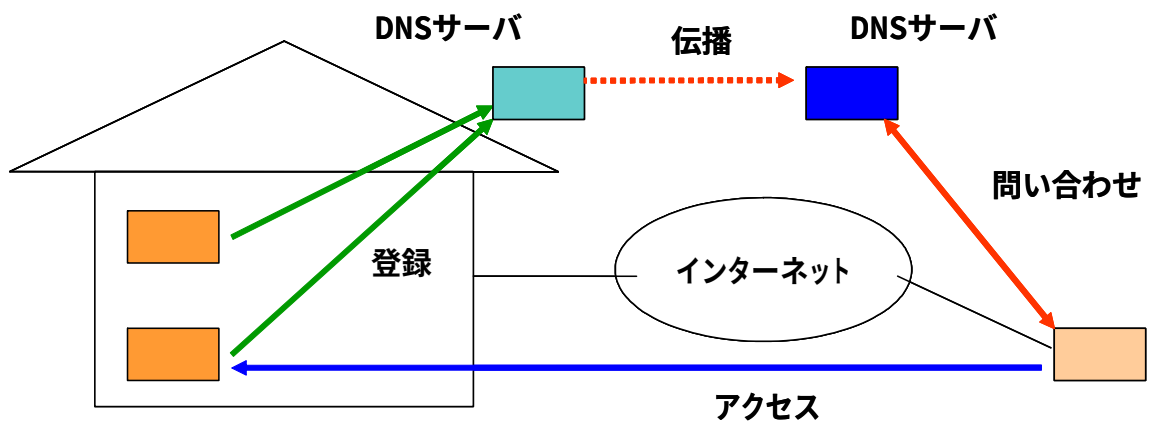
集中サーバ管理モデル

これは、契約に基づくサーバで管理するモデルです。登録済みノードのみアクセスが可能となります。登録は専用ソフトで行うことになるかもしれません。



既存DNSモデル

これは従来と同様、DNSサーバに登録する手法で、登録済みノードのみアクセス可能となります。登録方法は専用ソフトによる自動登録が行われるかもしれません。しかしこの場合、情報の公開範囲やプライバシーの問題への対処が課題です。



ネーミングのその他の課題

ネーミングに関するその他の課題としては、以下の点が挙げられます。

トランスポートプロトコルの選択

これはやはりデュアルスタックが望まれます。少なくともサーバ側は広く対応していることが好ましいと考えられます。ルータ(家庭用)へはいずれにせよデュアルスタックが搭載されるであろうことを考えると、デュアルスタックで問題はありません。

マルチプレフィックス／マルチホーム環境

IPv4 では PPPoE マルチセッションによって、マルチホームが実施されています。また、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ます。しかし、その設定は多くの場合、静的に行われます。IPv4 では NAT があるため、これまでマルチホームに関する問題は顕在化しませんでした。エンドノードはマルチホームを気にする必要がなかったのです。

しかし、IPv6 の場合、ソースアドレス選択が重要になります。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ります。

DNSSEC

また、DNS のセキュリティ確保のための DNSSEC が将来どのように利用されていくことになるかが未知数です。

non-PC機器への名前付け

PC ではない機器で、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という課題もあります。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求められます。特に家庭での配置と対応関係を持たせ、『玄関のカメラ』『リビングのエアコン』といった名前付けができることが望まれます。また、こうした名前付けのプロセスを、できれば自動化することが求められます。

改定履歴

2004 年版

新規発行

2005 年版

改訂項目

- ・ホームネットワークにおける移行シナリオへの追加
- ・名称の変更 “イベントに基づく”→“ホームネットワークにおける”
- ・B | R : IP ブリッジ搭載IPv4ルータの追加
- ・セキュリティ項目の詳細化
- ・プレイヤーにおけるシナリオの追加

移行WG Homeセグメント 検討メンバ

(敬称略)

2003 年度メンバ

SWGチェア

久保田 幸司 (松下電器)

検討メンバ (敬称略・50 音順)

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)

2004 年度メンバ

SWGチェア

岡 光秋 (東芝ソリューション)

久保田 幸司 (松下電器)

検討メンバ (敬称略・50 音順)

秋山 悟 (NTT西日本)

荒野 高志 (インテックネットコア)

石原 清輝 (KDDI)

石原 丈士 (東芝)
金山 健一 (インテックネットコア)
川島 正伸 (NEC アクセステクニカ)
後藤 邦泰 (富士通)
島田 裕一 (富士通アクセス)
瀬川 卓見 (パナソニックコミュニケーションズ)
滝澤 基行 (富士通アクセス)
古川 隆弘 (富士通アクセス)

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