IPv6 移行ガイドライン

(大企業・自治体セグメント)

2004 年 5 月

IPv6 普及・高度化推進協議会

移行 WG 大企業・自治体 SWG

目　次

はじめに.....1
■検討メンバー.....1
■お問い合わせ先.....1
1. セグメントの特徴.....2
■大企業・自治体ネットワークの特徴.....2
■大企業・自治体ネットワークの分類要素、IPv6 との関連性.....3
2. BCP（今すぐできること）.....4
■基本方針.....4
■BCP としてのセキュリティ.....5
■IPv6 ネットワーク構築のフロー.....6
■“今”IPv6 を導入する理由.....9
■ IPv6 ネットワーク環境の先行導入.....10
■新規アプリケーション導入に伴う IPv6 導入.....22
■具体的な IPv6 導入イメージ.....27
3. 5:5 段階に向けて.....35
■5:5 段階において想定される IPv6 利用環境と基本方針.....35
■段階置換型の場合.....36
■独立融合型の場合.....39
4. 5:5 に向かうための課題.....44
■マルチホーム.....44
■ネットワークアクセス制御.....45
■その他の 5:5 に向かうための課題（セキュリティ関連除く）.....46
5. セキュリティモデル.....47
■セキュリティに関する基本的な考え方.....47
■玄関モデルと金庫モデル.....48
■将来の F/W 構成.....49
■IPsec の F/W 越え.....50
6. Tips & Tricks.....54
■IPv6 ローカルアドレス付与方法.....54
■DNS サーバの設定.....55
■MTU ディスカバリについて.....57

はじめに

本ドキュメントは、大企業や自治体のネットワークを構築・運営するネットワーク管理者や SIer を対象に、大企業や自治体が今後 IPv6 を導入するにあたり、検討すべき一般的な項目、指針、方法について記述しています。

ここで記載される内容は、考え方の例を示すものであり、唯一の解ではありません。読者が、固有の運営方針や制約条件を前提に IPv6 の導入を検討する際、このドキュメントを参考に応用が図れるよう記述しました。

■検討メンバー

SWG チェア

月岡（日立製作所）
阪内（NEC）

検討メンバー

鈴木（日立製作所）
橘（あにあにどっとこむ）
田付（NEC）
徳重（NTT コミュニケーションズ）
中井（NTT コミュニケーションズ）
中原（NEC）
西田（リコー）
白田（日立製作所）
橋本（三菱総合研究所）
廣海（インテックネットコア）
山崎（NTT コミュニケーションズ）
山本（NTT 東日本）
吉岡（トヨタ IT 開発センタ）

（敬称略、あいうえお順）

■お問い合わせ先

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

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

1. セグメントの特徴

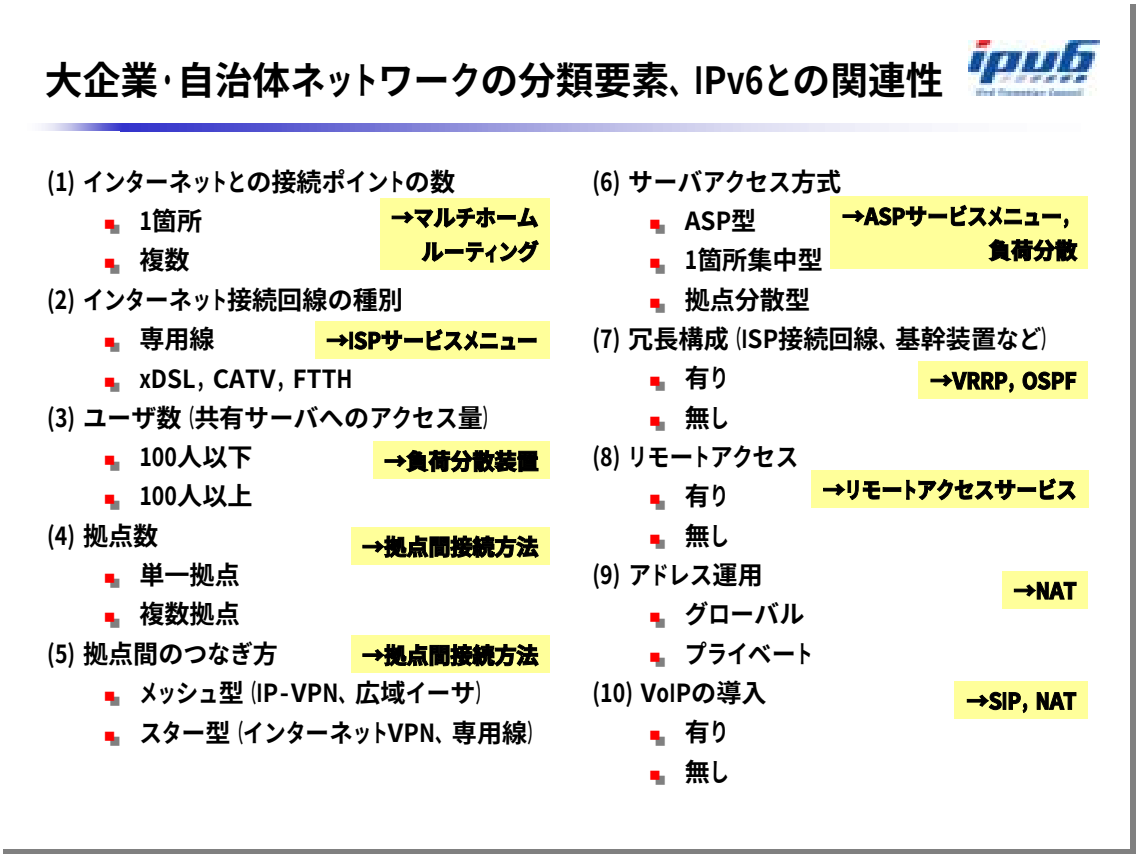
■大企業・自治体ネットワークの特徴

ここで対象とする大企業・自治体ネットワークの特徴として、以下の点が挙げられます。

まず、ユーザ数が数十人以上の比較的大規模なネットワークで、全体ネットワークを特定の専任部門が管理しています。組織内にイントラネットが存在しており、組織内部もしくは組織外部に対して、メール、Web などのアプリケーションサービスを提供しています。こうしたネットワークでは、費用対効果への考慮が特に強く求められます。

また、セキュリティについては、ネットワーク部門がポリシーを厳格に維持管理しています。さらに、ネットワーク設備に不具合が発生した場合、社会的・組織的に影響度が大きいことから、冗長構成や設備の定期更新が確実に行われています。

■大企業・自治体ネットワークの分類要素、IPv6 との関連性



大企業や自治体のネットワークは、上のような要素を基準として分類することができます。これらのポイントが、組織において可能な IPv6 への移行方法に影響を与えます。

2. BCP（今すぐできること）

■基本方針

まずは、IPv4 と同等の IPv6 ネットワーク環境の確立がターゲットとなります。ただし、当面は IPv4 も従来通り継続して運用し、徐々に IPv6 に切り替えていきます。ネットワークの使い分けかたとしては、既存アプリについては、無理に IPv6 化に固執する必要は無く、既存 IPv4 ネットワークシステムで継続運用し、バージョンアップなどのついでに可能であれば IPv6 化すると良いでしょう。新規に導入するアプリについては、将来的観点でも極力新規 IPv6 ネットワークシステムで導入することとし、十分に試行した後、実運用化します。

導入方法は、当初、必要最低限の範囲の中で、IPv4/IPv6 デュアルスタックネットワークを構築し、部分的に IPv6 を導入した場合は、IPv6 over IPv4 トンネリングによって相互接続します。その後、定期更新やネットワーク利用ニーズの発生に応じて、徐々に IPv6 対応範囲を拡大していく方法をとります。

■BCP としてのセキュリティ

大企業・自治体ネットワークにおいては、とりわけ厳格なネットワークセキュリティの確保が前提となります。これを踏まえた、当面の暫定的なセキュリティに関する方針としては、次の 2 通りが考えられます。

緩和モデル

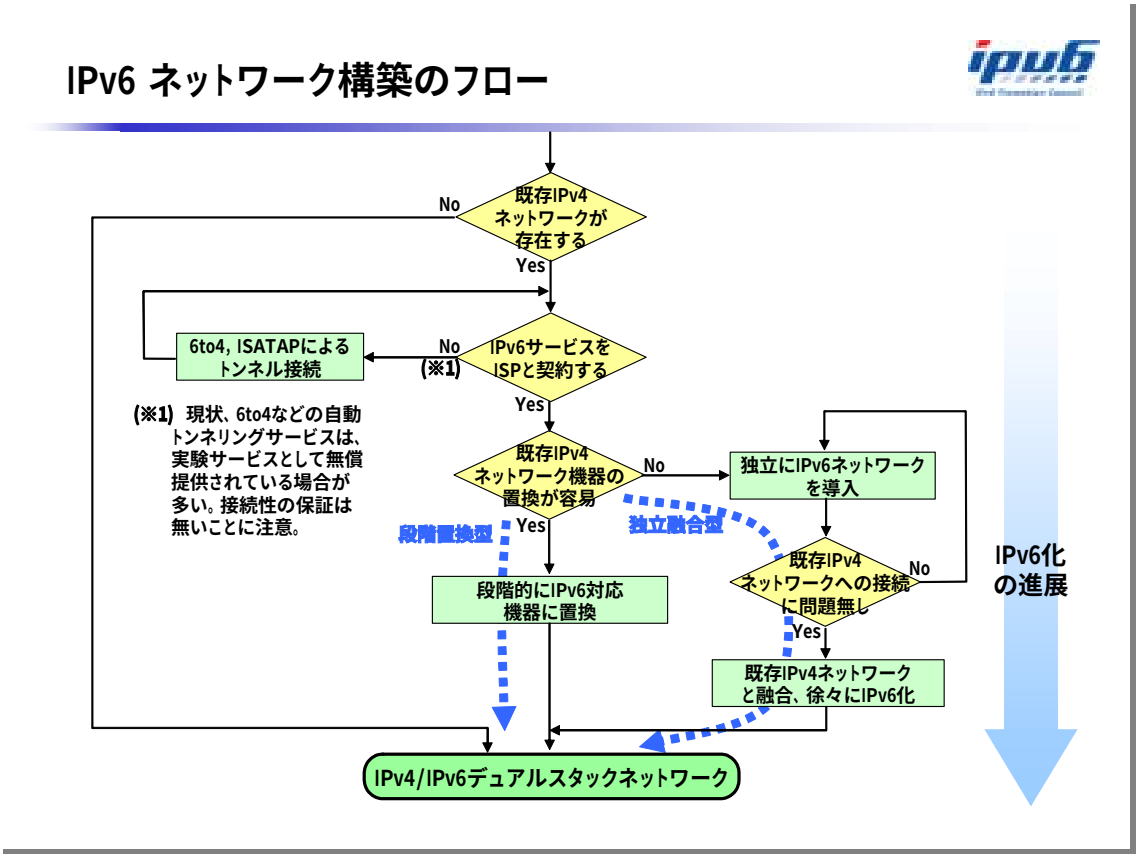
この場合、現状の IPv4 ベースのファイアウォール設定に、IPv6 対応の設定を同等レベルで設定し、さらに追加設定として、個別の IPv6 アクセスを限定的に許可します。第一段階で、一部セグメントを IPv6 化（トンネリング接続なども含む）します。IPv6 アプリケーションの P2P アクセスなどについては、特別に検討の上で、ファイアウォールに最低限の穴を開けるかどうかを判断します。

厳格モデル

このモデルでは、既存ネットワークと新規 IPv6 ネットワークの接続を認めないことをセキュリティポリシーとします。第一段階で、現用ネットワークとは独立した IPv6 ネットワークを構築します。大企業・自治体の IPv6 セキュリティポリシーが、さらに実用的なレベルまで確立されるまでは、IPv6 ネットワークおよびこれに接続する端末上で、企業秘密情報、個人情報などの取り扱いは控えたほうが良いでしょう。

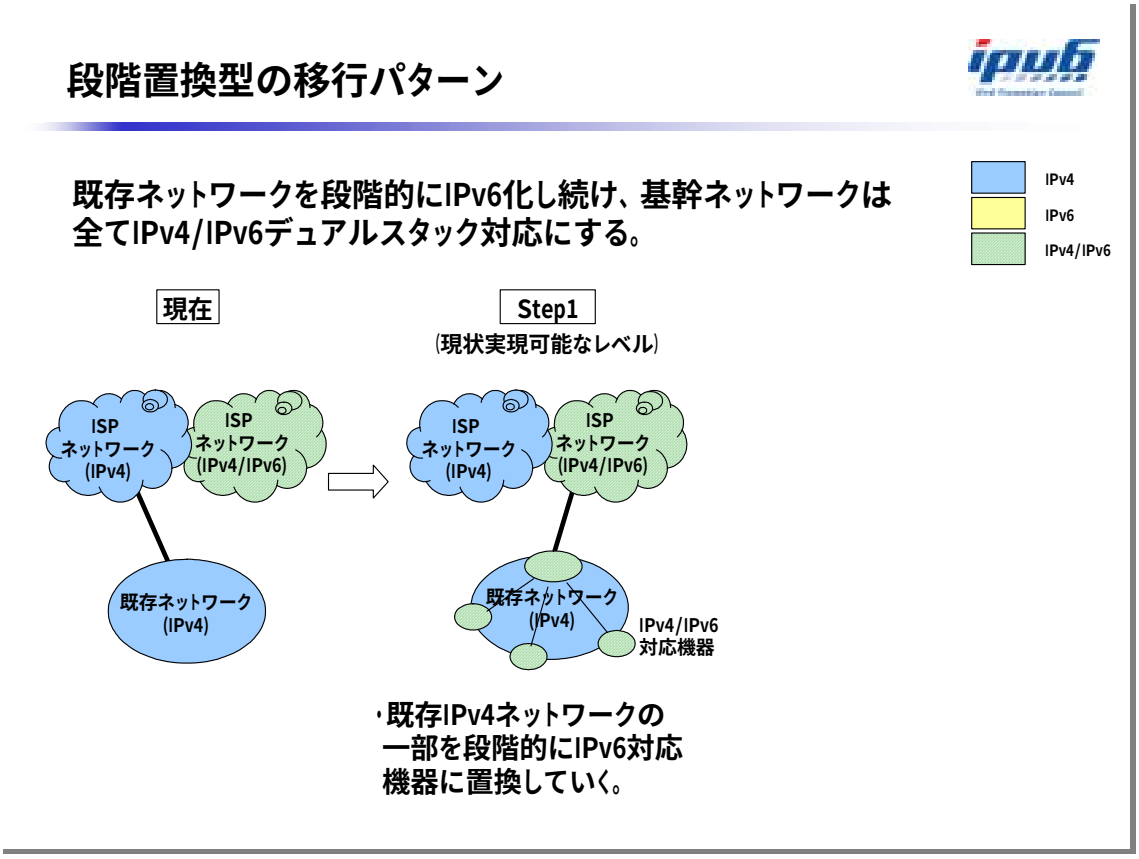
いずれにしても、大企業や自治体にとって、“ IPv6 セキュイティポリシーの整理は、直近の最重要課題である！ ”と言えます。

■IPv6 ネットワーク構築のフロー



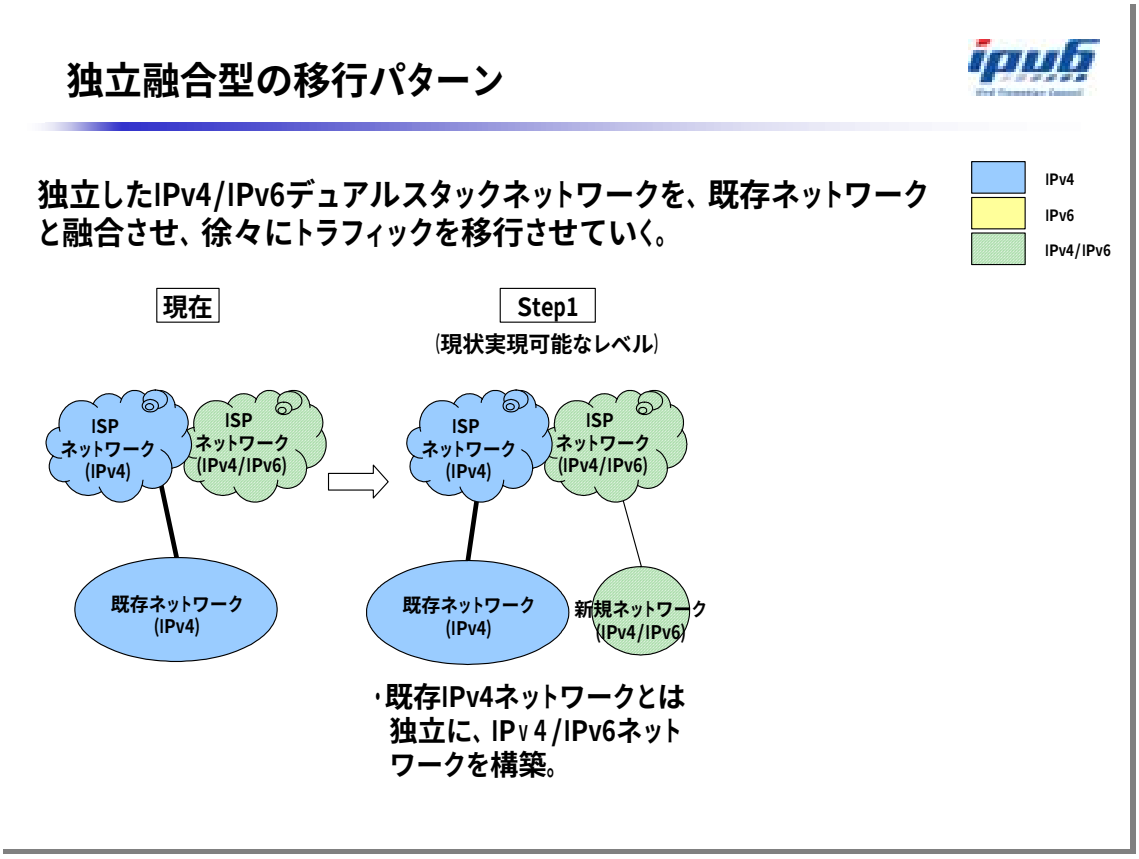
企業における IPv6 移行は、図のように模式化されます。IPv6 の移行は、段階置換型と独立融合型の 2 つのタイプに分けることができます。また、これらの 2 タイプによる移行の前に、IPv6 接続サービスと契約することなく IPv6 ネットワークを試してみることも可能です。

(1) 段階置換型の移行パターン



これは、既存の IPv4 ネットワークを、段階的に IPv4 と IPv6 のデュアルスタック環境に移行していくものです。徐々にデュアルスタックの部分を拡大していき、最終的にはネットワークの大部分をデュアルスタック化することを目指します。

(2) 独立融合型の移行パターン



これは、既存の IPv4 ネットワークと独立したデュアルスタックネットワークを構築し、既存ネットワークと融合し、徐々にトラフィックを移行していくパターンです。

■“今”IPv6 を導入する理由

大企業が現在の段階で IPv6 を導入しようと考える理由は、以下のものが考えられます。

1. IPv6 ネットワーク環境の先行導入
   長期的な設備計画に基づいて IPv6 を先行導入し、将来のネットワークアプリケーションを先取りする。
2. 新規アプリケーション（VoIP など）導入に伴う IPv6 導入
   出張、会議などの業務効率改善。在宅勤務の可能性。
   組織→個人単位のセキュリティ管理。
3. IPv6 開発のための環境整備
   IPv6 関連製品の開発自体が目的。
4. 企業イメージ／プレゼンス、営業力／顧客アピール力の向上
   先進技術の導入により、企業イメージの向上が期待できる。

■ IPv6 ネットワーク環境の先行導入

(1) IPv6 対応サービス・機器について

IPv6 を利用するための基本的要素技術はすでに整っていると言えます。

ISP 接続回線

主要 ISP はすでにトンネル方式、デュアルスタック方式、ネイティブ方式の 3 方式で商用サービスを提供開始しています。この 3 方式のうち、とりあえず IPv6 を体験するならトンネル方式が適しています。既存 IPv4 ネットワークへの影響が最小限で済むからです。ただし、カプセリングによるオーバーヘッドは覚悟すべきです。

本格的な IPv6 導入を想定するならデュアルスタック方式を選択すべきです。いきなり IPv6 オンリーのネイティブ回線は、DNS、SNMP などにおける IPv6 対応が完了していないことから、現状では利用における制約の多い選択肢です。ネイティブ回線は、おもに小規模 ISP 向けサービスと考えたほうがよいでしょう。

ルータ

中～大規模ルータのほとんどは IPv6 対応済みです（ハードウェア処理対応も進展）。ベンダー間の相互接続性も高く、RIPng、OSPFv3、PIM-SM などのプロトコルで相互接続検証が進んでいます。一方、小型ルータの IPv6 対応が意外に遅れているという状況があります。IPv4 と IPv6 とは独立にコンフィギュレーションが可能であることも考慮すると、ルータの IPv6 対応は、今や必須条件と言えるかもしれません。

ファイアウォール

商用ファイアウォールでは、ようやく基本的なパケットフィルタリング機能が IPv6 対応しはじめた段階です。機能、性能、信頼性に関する検証は必要です。

クライアント端末同士の P2P アプリや IPsec 通信、トンネリングやマルチキャストに対するセキュリティポリシーをどのように設定するべきかは、今後の大きな課題です。現状のファイアウォールでは、マルチキャストルーティングプロトコルに対応した製品が存在しません。

DNS サーバ

BIND を使っていれば、標準的なバージョンアップで IPv6 化が可能です。デュアルスタックのネットワークであれば、AAAA レコード対応が重要であり、DNS 問い合わせパケットの IPv6 化にまでこだわる必要はありません。暫定的には、内部で IPv6 対応 DNS を立てるのではなく、IPv6 対応の外部 DNS を参照する手段も考えられるかもしれません。

その他のサーバ

Web サーバやメールサーバなどは、IPv6 対応が進んでいます。ただしサーバの IPv6 化においては、ウィルスチェックアプリケーションの IPv6 対応について別途確認し、セキュリティ対策も考慮した検討が必要です。ネットワーク管理サーバは、MIB が IPv6 対応しています。SNMP は IPv4 ベースに留まっている製品がほとんどです。

PC・PDA

主要な OS は、ほぼ IPv6 対応済みです。しかし、機能的な対応レベルは様々です。企業においては、新規購入や OS の最新化に伴い IPv6 化が進むと考えられます。しかし、エンドツーエンド通信を考慮して、端末レベルでのセキュリティ対策（パーソナルファイアウォールやウィルススキャンソフトなどの導入）を徹底する必要があります。

(2) IPv6 グローバルアドレスの取得と運用

IPv6 アドレスの取得方法

企業は、IPv6 サービスを提供している ISP（商用、試験サービスを含め多数）と契約することにより、/48、もしくは/64 のグローバル・プレフィックスの割り当てを受けることが可能です。大企業・自治体ネットワークとして一定規模のネットワークを構成するにあたっては/48 の IPv6 アドレスを取得することを推奨します。導入初期段階で、ISP からグローバルアドレスを取得する前に、試行的に閉域で IPv6 を導入する場合のアドレス付与方法については、6 章 Tips の「IPv6 ローカルアドレス付与方法」を参照してください。

IPv6 アドレス設計・運用方法

/48 のグローバル・プレフィックスは、ほとんどの大企業・自治体ネットワークにとって十分なアドレス空間です。

IPv4 では、セグメント分割する時に将来接続が予想される端末数を綿密に考慮の上でアドレス設計する必要があります。一方、IPv6 の場合は、下位 64bit のインタフェース識別子により実質的に端末が無限に接続可能なため、/48 のグローバルアドレスを取得した場合、端末数を意識せずに 16bit を使用してセグメント分割のアドレス設計が可能です。

しかし、将来の展開を考慮して下記の項目に留意すべきです。

・シンプルで効率のよい（見やすい）アドレスの割付け
・将来予想されるネットワーク構成の組み換え・拡大を想定した、計画的なアドレス割付け
・対象ネットワークにおける地理的・組織的な構成に合わせたアドレス割付け

(3) ルーティング

機器の対応現状

ほとんどの IPv6 対応ルータは RIPng 対応済みです。上位機種では、OSPFv3 にも対応しています。他社互換性の検証も実施されており、実用的にも問題はありません。

IPv6 ルーティングプロトコル

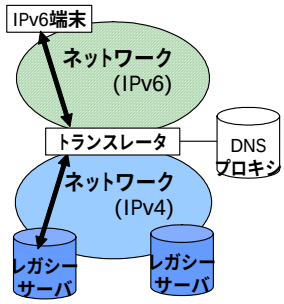
大企業・自治体ネットワークにおいて、IPv6 導入当初はスタティックルーティングで十分です。規模拡大に応じて、RIPng や OSPFv3 を導入するのも良いでしょう。デュアルスタック時には、IPv4 のルーティングプロトコルと合わせた方が分かりやすいと言えます。ライブ中継や放送などのサービスでマルチキャストの利用を想定する場合は、PIM-SM などのマルチキャストルーティングプロトコルに対応した機器を選択する必要があります。

(4)トランスレータ

トランスレータ

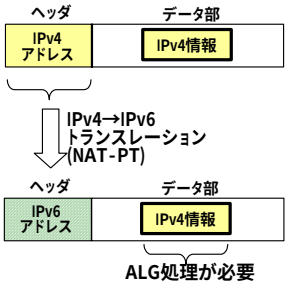
＜特徴＞

- NAT-PT方式、TRT方式が商用化されている。
- 通信の途中でプロトコル変換を実施することにより、IPv4ホストとIPv6ホストとの間での通信を実現。
- DNSプロキシを利用して、FQDN（Fully Qualified Domain Name）を使って通信相手を指定可能。
- レガシーシステムのサーバ設定を変更することなく、IPv6対応にすることが出来る。（膨大なIPv4システムの資産をそのまま利用可能。）



＜問題点＞

- 階層違反のあるアプリケーションには、ALG（Application Level Gateway）が必要。（右図参照）
- IPv4→IPv6パケット変換時は、MTU（Maximum Transmission Unit）の設定にも要注意。
- 通信相手にはFQDNが必要。
- リバースプロキシによるプロトコル変換との使い分け。



特徴

主に NAT-PT 方式、TRT 方式のトランスレータが商用化されています。通信の途中で IPv4/IPv6 プロトコル変換を実施することにより、IPv4 ホストと IPv6 ホストとの間での通信を実現します。DNS プロキシを利用して、FQDN（Fully Qualified Domain Name）を使って通信相手を指定可能です。レガシーシステムのネットワーク設定を変更することなく、IPv6 対応にすることができます（膨大な IPv4 システムの資産をそのまま利用可能）。

問題点

階層違反のあるアプリケーションには、ALG（Application Level Gateway）が必要です。IPv4→IPv6 パケット変換時は、MTU（Maximum Transmission Unit）の設定にも注意する必要があります。通信相手には FQDN が必要です。リバースプロキシによるプロトコル変換との使い分けが求められます。

(5) トンネリング

固定トンネリング

特定の IPv6 対応ルータ間で固定的に IPv6 over IPv4 トンネルを生成します。

自動トンネリング

●DTCP（Dynamic Tunnel Configuration Protocol）

クライアント側から動的にトンネル生成を要求可能です（例：フリービット Feel6 Farm

IPv6 接続実験)。

●6to4

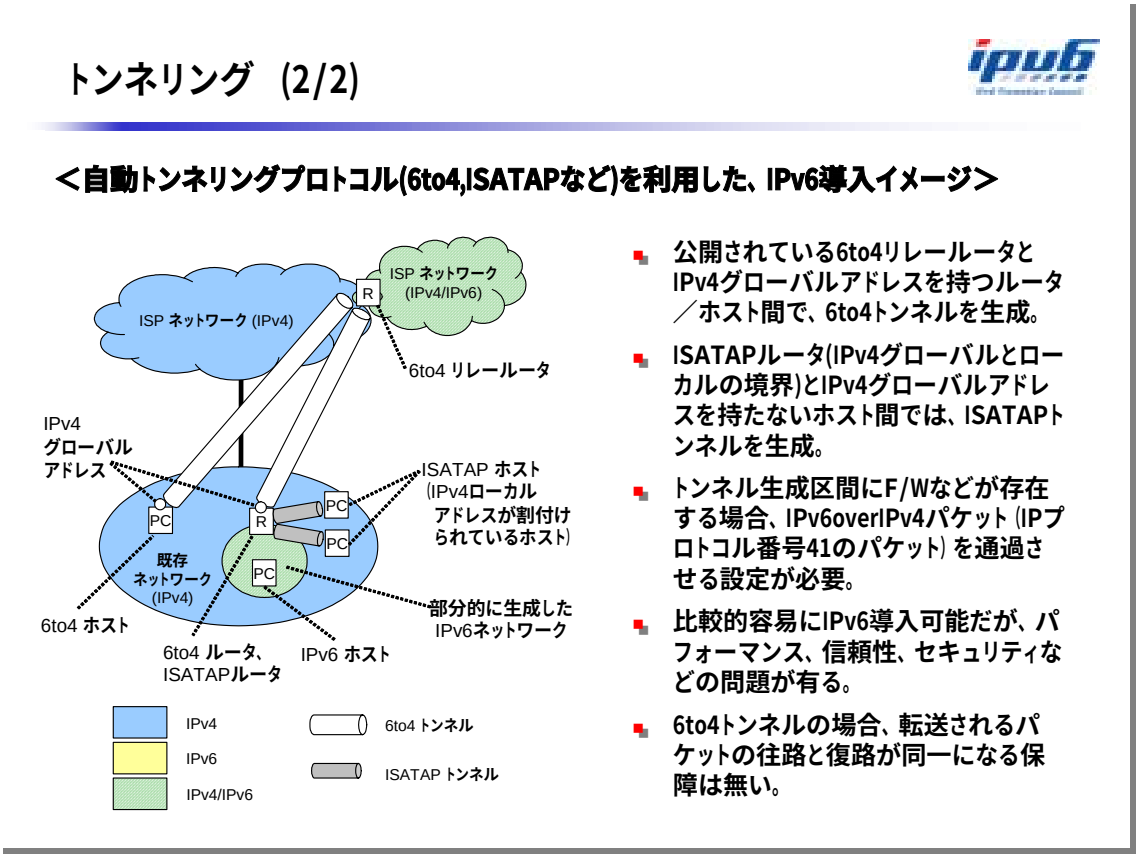
グローバル IPv4 アドレスから IPv6 アドレスを自動生成します。Windows XP では、ホストにグローバル IPv4 アドレスが付与されると、自動的に 6to4 トンネルが生成されます。主要 ISP などが供給する 6to4 リレールータとの間でトンネルを張りますが、往路と復路の経路が同一になる保障はありません。

●ISATAP

ローカル IPv4 アドレスが運用されている LAN の中でトンネルを生成可能です。

●Teredo

NAT デバイスが介在する環境においてトンネル技術を利用可能です。



自動トンネリングプロトコルは、次のように利用できます。

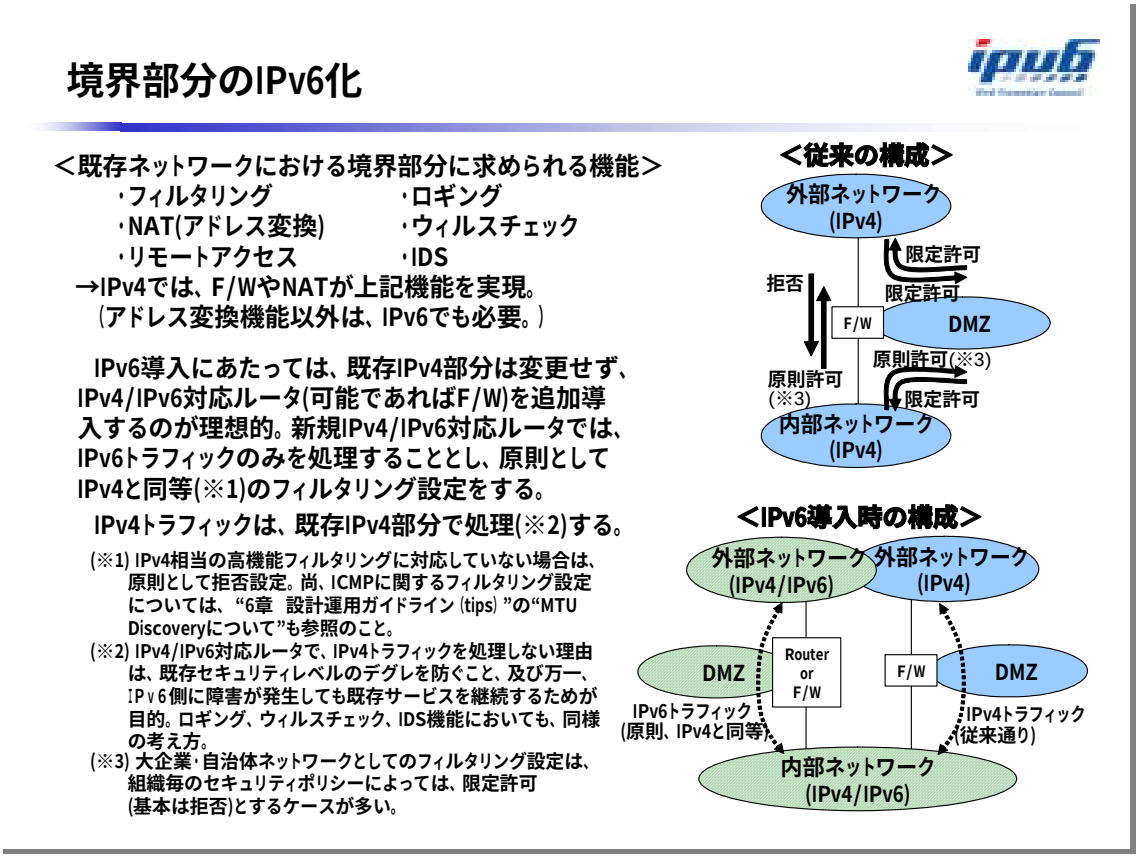
・公開されている 6to4 リレールータと IPv4 グローバルアドレスを持つルータ／ホスト間で、6to4 トンネルを生成

・ISATAP ルータ(IPv4 グローバルとローカルの境界)と IPv4 グローバルアドレスを持たないホスト間では、ISATAP トンネルを生成

注意点としては、これらの自動トンネルプロトコルを使うと、比較的容易に IPv6 の導入が可能となりますが、パフォーマンス、信頼性、セキュリティなどの問題があります。特にトンネル区間にファイアウォールなどが存在する場合、IPv6overIPv4 パケット（IP プロトコル番号 41 のパケット）を通過させる設定が必要となりますが、その場合にセキュリティ管理

上問題が無いかを十分検討する必要が有ります。また、6to4 トンネルの場合、転送されるパケットの往路と復路が同一になる保障はありません。

(6) 境界部分の IPv6 化



既存ネットワークで境界部分に求められてきた機能としては、フィルタリング、ロギング、NAT(アドレス変換)、ウィルスチェック、リモートアクセス、IDS などがあり、IPv4 では、ファイアウォールや NAT 装置がこれらの機能を実現してきました。IPv6 においても、NAT（アドレス変換機能）以外は必要な機能です。IPv6 導入にあたっては、既存 IPv4 部分は変更せず、IPv4/IPv6 対応ルータ（可能であればファイアウォール）を追加導入するのが理想的です。新規 IPv4/IPv6 対応ルータでは、IPv6 トラフィックのみを処理することとし、原則として IPv4 と同等(※1)のフィルタリング設定をします。IPv4 トラフィックは、既存 IPv4 部分で処理(※2)します。

(※1) IPv4 相当の高機能なフィルタリングに対応していない場合は、原則として拒否設定。なお、ICMP に関するフィルタリング設定については、「設計運用ガイドライン（tips）」の“ MTU Discovery について ”も参照してください。

(※2) IPv4/IPv6 対応ルータで、IPv4 トラフィックを処理しない理由は、既存セキュリティレベルの低下を防ぐことと、万一 IPv6 側に障害が発生しても既存サービスを継続できるようにするためです。ロギング、ウィルスチェック、IDS 機能においても、同様の考え方をとります。

(※3) 大企業・自治体ネットワークとしてのフィルタリング設定は、組織毎のセキュリティポリシーによっては、限定許可(基本は拒否)とするケースが多くみられます。

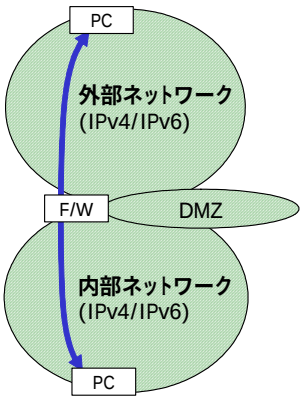
(7) フィルタリング

フィルタリング（1） ～IPv6対応F/Wの場合～

現状においては、IPv4とIPv6で同等のセキュリティポリシーを維持する（もしくは、デグレがないようにする）のが基本。

＜E2E通信について＞

- **F/Wを経由するE2E通信を許容する場合、限定した端末において特定のアクセス(IPアドレス、ポート番号でフィルタリング)のみを通過させるべき。**
- **F/Wを経由するIPsecベースのE2E通信は、今後の課題。（試験的に許容する場合は、限定した端末において特定のアクセス(IPアドレスでフィルタリング)のみを通過させるべき。その際、終端装置には、パーソナルF/Wなどのセキュリティ対策を導入すべき。）**



IPv6 対応 F/W の場合

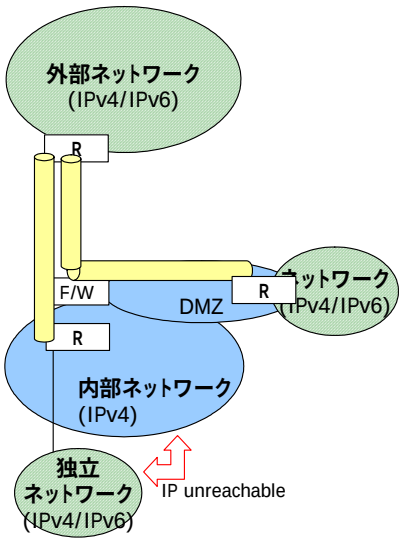
IPv6 対応ファイアウォールを利用する場合、現状においては、IPv4 と IPv6 で同等のセキュリティポリシーを維持する（もしくは、セキュリティレベルの低下がないようにする）のが基本です。ファイアウォールを経由するエンドツーエンド通信を許容する場合、限定した端末において特定のアクセス（IP アドレス、ポート番号でフィルタリング）のみを通過させるべきです。ファイアウォールを経由する IPsec ベースのエンドツーエンド通信をどう扱うかについては、今後の課題となります（試験的に許容する場合は、限定した端末において特定のアクセス(IP アドレスでフィルタリング)のみを通過させるべきです。その際、終端装置には、パーソナル F/W などのセキュリティ対策を導入すべきです）。

IPv6 未対応 F/W の場合

フィルタリング（2） ～IPv6未対応F/Wの場合～

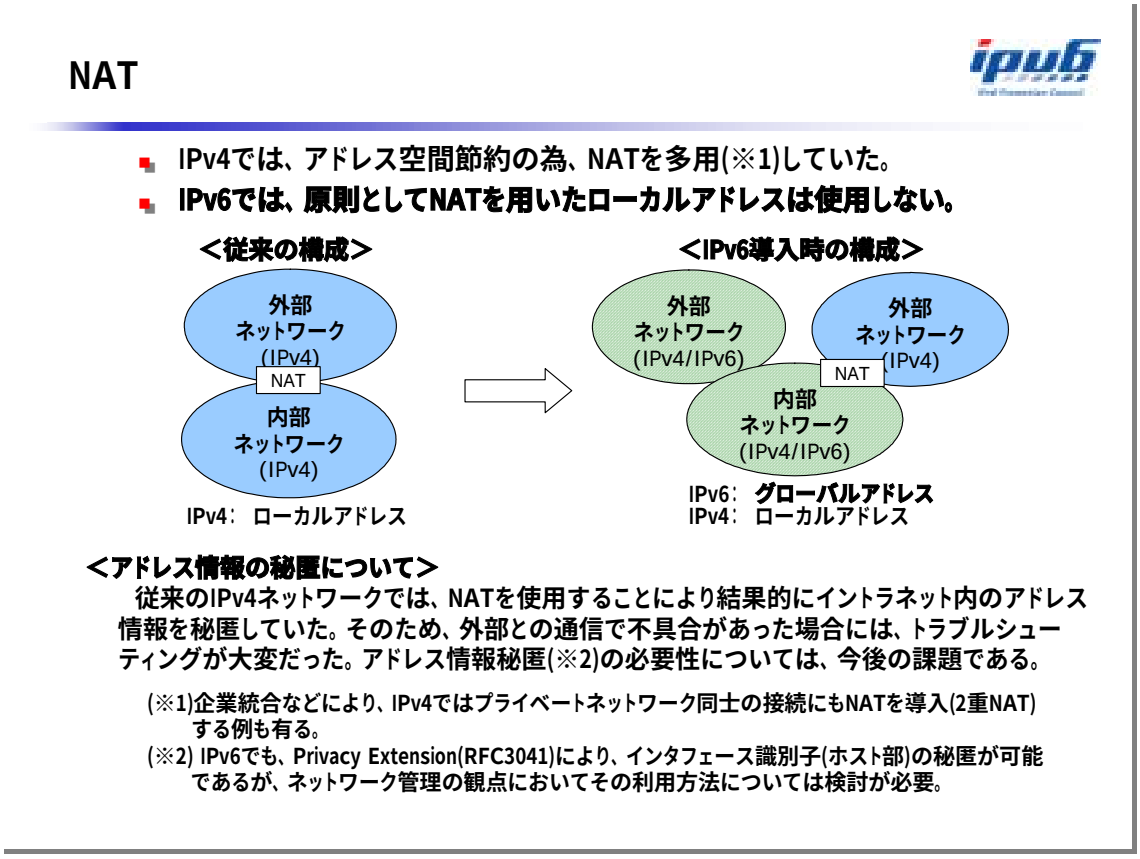
＜IPv6overIPv4トンネルについて＞

- **基本は、IPv6overIPv4トンネリングアクセスをDMZ向けに対して許可（IPプロトコル番号41の通過を許可）し、DMZにおける部分的なIPv6対応セグメントを生成します。このIPv6対応セグメントでは接続ホストを限定し、特別なセキュリティ管理を実施すべき。**
- **IPv6overIPv4トンネル通信を内部ネットワークへ許可（IPプロトコル番号41を通過）する場合は、当面は既存ネットワークとは独立したネットワーク（IP unreachable）で試行すべき。**



IPv6 に未対応のファイアウォールを使う場合、基本的には、IPv6overIPv4 トンネリングアクセスを DMZ 向けに対して許可（IP プロトコル番号 41 の通過を許可）し、DMZ において部分的な IPv6 対応セグメントを生成します。この IPv6 対応セグメントでは接続ホストを限定し、特別なセキュリティ管理を実施するべきです。IPv6 over IPv4 トンネル通信を内部ネットワークへ許可（IP プロトコル番号 41 を通過）する場合は、当面は既存ネットワークとは独立したネットワーク（相互に IP unreachable な形）で試行すべきです。

(8) NAT



IPv4 ではアドレス空間節約のため、NAT を多用していました(※1)。しかし、IPv6 では原則として、ローカルアドレス及び NAT は使用しません。

従来の IPv4 ネットワークでは、NAT を使用することにより結果的にイントラネット内のアドレス情報を秘匿していました。そのため、外部との通信で不具合があった場合にはトラブルシューティングが大変でした。アドレス情報秘匿(※2)の必要性については、今後の課題となります。

また、システム管理者がグローバルアドレスを用いることについて漠然とした不安を抱くという導入のバリアがよく指摘されますが、実際には米国などでは CIDR 以前に取得したグローバルアドレスを用いてイントラネットを構築している例も少なくありません。不安の解消するための方策は別途検討する必要があります。

(※1) 企業統合などにより、IPv4 ではプライベートネットワーク同士の接続にも NAT を導入(2 重 NAT)する例もあります。

(※2) IPv6 でも、Privacy Extension(RFC3041)により、インタフェース識別子(ホスト部)の秘匿が可能ですが、ネットワーク管理の観点では、その利用方法については十分な検討が必要です。

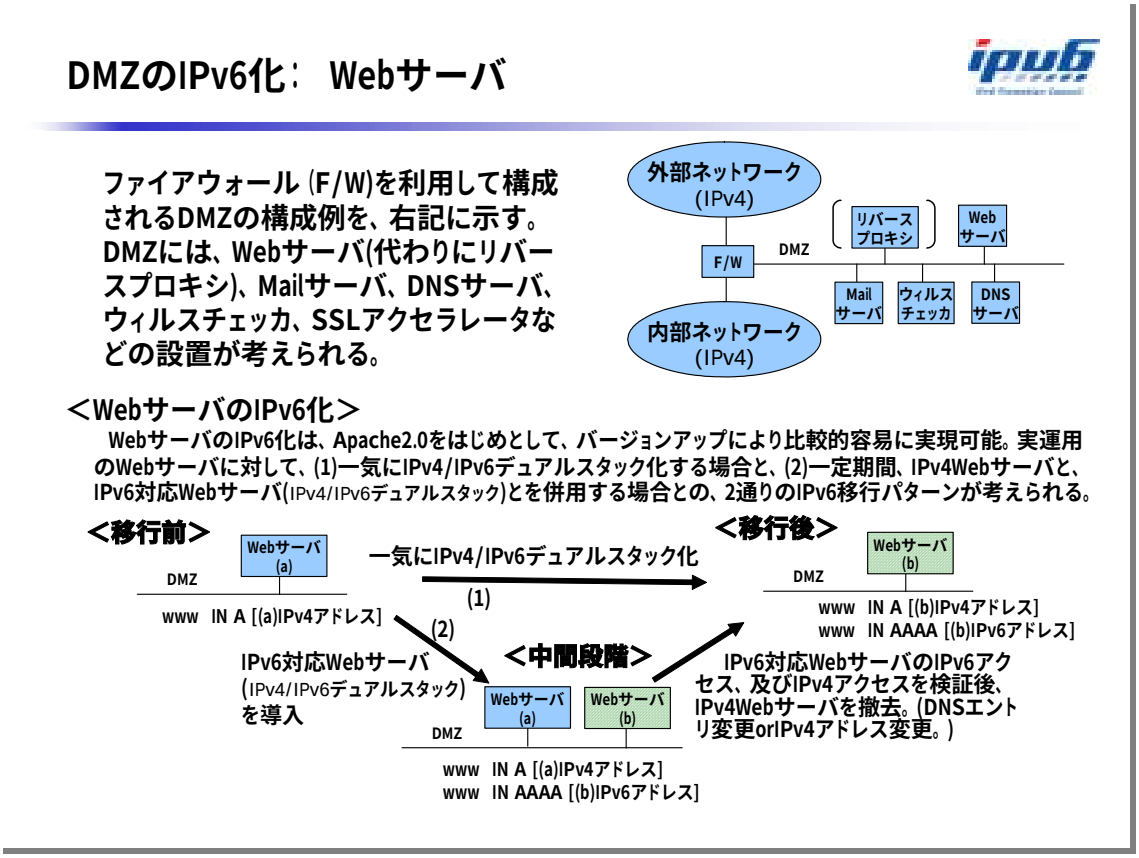
(9)リモートアクセス

現状のリモートアクセス方式は、以下の 4 通りに分類されます。

1. （企業が持つ）NAS に電話をかける
2. （プロバイダが持つ）NAS に電話をかけて、そこから一括して L2TP でアクセス
3. インターネット VPN（トンネルモード）
4. SSL-VPN

IPv6 によるリモートアクセスを実現するには、IPv4 でのリモートアクセス上で、IPv6 トンネルを張るのが最も現実的です。ただし、IPv6 over IPv4 over IPv4（セキュリティトンネル）となるため、フラグメンテーション問題についても特に注意する必要があります。

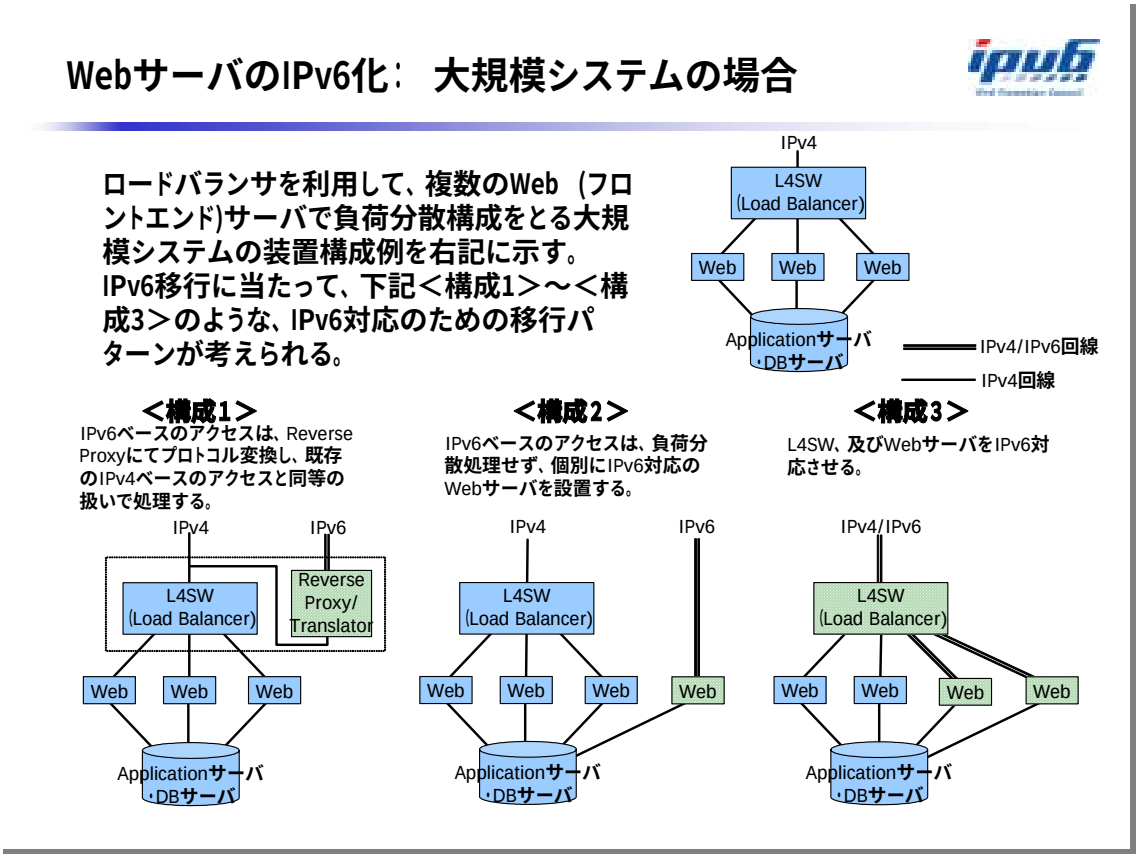
(10) DMZ の IPv6 化： Web サーバ



ファイアウォールを利用して構成される DMZ の構成例を、図に示します。DMZ には、Web サーバ(またはその代わりにリバースプロキシ)、メールサーバ、DNS サーバ、ウィルスチェッカ、SSL アクセラレータなどの設置が考えられます。

Web サーバの IPv6 化は、Apache2.0 をはじめとして、バージョンアップにより比較的容易に実現可能です。実運用の Web サーバに対して、(1)一気に IPv4/IPv6 デュアルスタック化する場合と、(2)一定期間、IPv4Web サーバと、IPv6 対応 Web サーバ(IPv4/IPv6 デュアルスタック)とを併用する場合との、2 通りの IPv6 移行パターンが考えられます。

(11) Web サーバの IPv6 化： 大規模システムの場合



ロードバランサを利用して、複数の Web(フロントエンド)サーバで負荷分散構成をとる大規模システムの装置構成例を図に示しました。IPv6 移行にあたって、構成 1～3 のような、IPv6 対応のための移行パターンが考えられます。

(12) 拠点間接続方式

拠点間接続方式

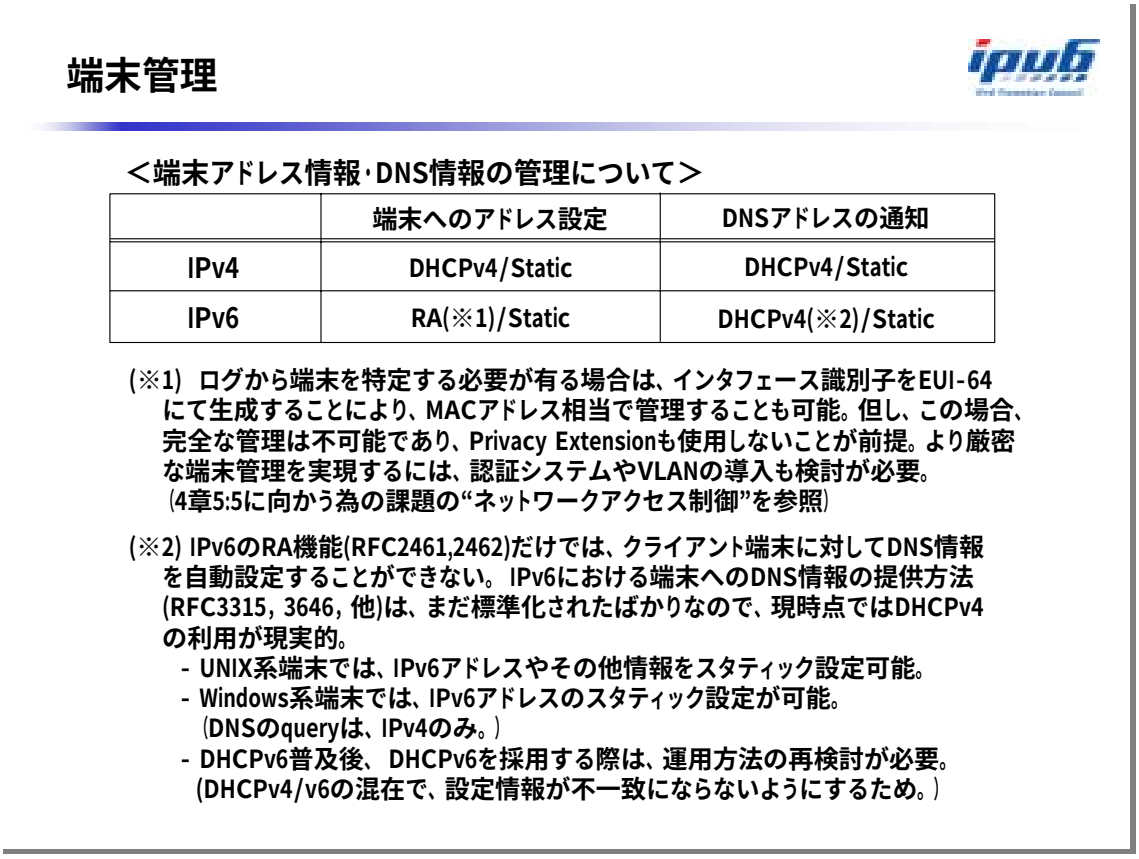
	デュアル(IPv4/IPv6)	トンネル(IPv6overIPv4)
フレームリレー	○(※1)	○
専用線	○(※1)	○
IP-VPN	ー(※2)	○
広域Ether	○(※1)	○

(※1)：終端装置のIPv6化で対応可能（IP非依存のはず。但し、サービス提供者へ確認必要。）
(※2)：現状IPv6対応しているサービス無し。

・IPv6導入初期段階では、トンネルによるIPv6対応が現実的。
・トラフィックの負荷などが切迫してきた時点で、デュアルスタック対応の新しいサービスメニューを検討。
・IPv6導入に伴う、新規IPv6アプリケーションや、既存IPv4アプリケーションのQoS維持/管理については、各々の拠点間接続サービス毎の回線提供事業者への確認が必要。

IPv6 導入初期段階では、トンネルによる IPv6 対応が現実的です。トラフィックの負荷などが切迫してきた時点で、デュアルスタック対応の新しいサービスメニューを検討すべきです。IPv6 導入に伴う、新規 IPv6 アプリケーションや、既存 IPv4 アプリケーションの QoS 維持/管理については、各々の拠点間接続サービス毎の回線提供事業者への確認が必要となります。

(13) 端末管理



端末管理

＜端末アドレス情報･DNS情報の管理について＞

	端末へのアドレス設定	DNSアドレスの通知
IPv4	DHCPv4/Static	DHCPv4/Static
IPv6	RA(※1)/Static	DHCPv4(※2)/Static

(※1) ログから端末を特定する必要が有る場合は、インタフェース識別子をEUI-64にて生成することにより、MACアドレス相当で管理することも可能。但し、この場合、完全な管理は不可能であり、Privacy Extensionも使用しないことが前提。より厳密な端末管理を実現するには、認証システムやVLANの導入も検討が必要。
（4章5:5に向かう為の課題の“ネットワークアクセス制御”を参照）

(※2) IPv6のRA機能(RFC2461,2462)だけでは、クライアント端末に対してDNS情報を自動設定することができない。IPv6における端末へのDNS情報の提供方法(RFC3315, 3646, 他)は、まだ標準化されたばかりなので、現時点ではDHCPv4の利用が現実的。
- UNIX系端末では、IPv6アドレスやその他情報をスタティック設定可能。
- Windows系端末では、IPv6アドレスのスタティック設定が可能。
（DNSのqueryは、IPv4のみ。）
- DHCPv6普及後、DHCPv6を採用する際は、運用方法の再検討が必要。
(DHCPv4/v6の混在で、設定情報が不一致にならないようにするため。)

ログから端末を特定する必要が有る場合は、インタフェース識別子を EUI-64 から生成することにより、MAC アドレス相当で管理することも可能です。但し、インタフェース識別子は自由に個別設定可能なため、完全な管理は不可能です。また、Privacy Extension も使用しないことが前提となります。より厳密な端末管理を実現するには、認証システムと VLAN を組み合わせたシステムの導入を検討する必要があります（4 章 5:5 に向かうための課題の“ ネットワークアクセス制御 ” を参照）。

IPv6 の RA 機能（RFC2461、2462）だけでは、クライアント端末に対して DNS 情報を自動設定することができません。IPv6 における端末への DNS 情報の提供方法（RFC3315, 3646, 他）は、まだ標準化されたばかりなので、現時点では DHCPv4 の利用が現実的です。

・UNIX 系端末では、IPv6 アドレスやその他情報をスタティックに設定可能です。
・Windows 系端末では、IPv6 アドレスのスタティック設定が可能です（DNS クエリは、IPv4 のみ）。
・DHCPv6 普及後、DHCPv6 を採用する際は、運用方法の再検討が必要です（DHCPv4/v6 の混在で、設定情報が不一致にならないようにするため）

■新規アプリケーション導入に伴う IPv6 導入

(1) アプリケーションの IPv6 対応の進め方

アプリケーションのIPv6対応の進め方

＜IPv6アプリケーション導入にあたっての基本的考え方＞

- 新規アプリケーションについては、原則としてIPv4/IPv6デュアルスタック対応とする。
- 既存アプリケーションは、無理にIPv6に対応させる必要は無い。
  - ソフトウェアバージョンアップのついでにIPv6化。(※1)
  - フロントアプリケーションが存在する場合は、フロントアプリケーションを優先してIPv6化。

(※1)：但し現時点では、例えばMailサーバのIPv6化においては、ウィルスチェックアプリケーションのIPv6対応について別途確認し、セキュリティ対策も考慮した検討が必要。

- ＜開発者向け＞：アプリケーションはプロトコル非依存の枠組みで開発する。
  - Socketを使うだけでなく、RPCなどのアプリケーションに依存しないインターフェイスの利用も検討することが望ましい。

＜IPv6らしいアプリケーションとは？＞ →やはり、P2Pアプリケーション？

P2Pアプリケーション	イントラ内	外部(特定)	外部(不特定)
VoIP	○	○	○
IM(インスタントメッセンジャ)	○	○	○
グループウェア	○	○	ー
サーバレス ファイル共有	○	○	ー
メンテナンス／モニタリング	○	○	ー
マルチキャストストリーミング	○	ー	ー
固定アドレス (MIP)	○	○	ー
テレビ会議	○	○	ー

新規アプリケーションについては、原則として IPv4/IPv6 デュアルスタック対応とすべきです。既存アプリケーションは、無理に IPv6 に対応させる必要はありません。ソフトウェアバージョンアップのついでに IPv6 化するのがよいと思われます。現時点では、たとえば Mail サーバの IPv6 化においては、連携することとなるウィルスチェックアプリケーションの IPv6 対応が必要性などについて別途確認し、セキュリティ対策を重視した検討が必要です。フロントアプリケーションが存在する場合は、フロントアプリケーションを優先して IPv6 化します（内部側ネットワークの IPv6 化を優先する必要はありません）。

アプリケーションはプロトコル非依存の枠組みで開発します。Socket を使うだけでなく、RPC などのアプリケーションに依存しないインタフェースの利用も検討することが望ましいと思われます。

IPv6 にふさわしいアプリケーションの例を表に掲げます。やはり P2P アプリケーションが IPv6 らしいと言えるでしょう。

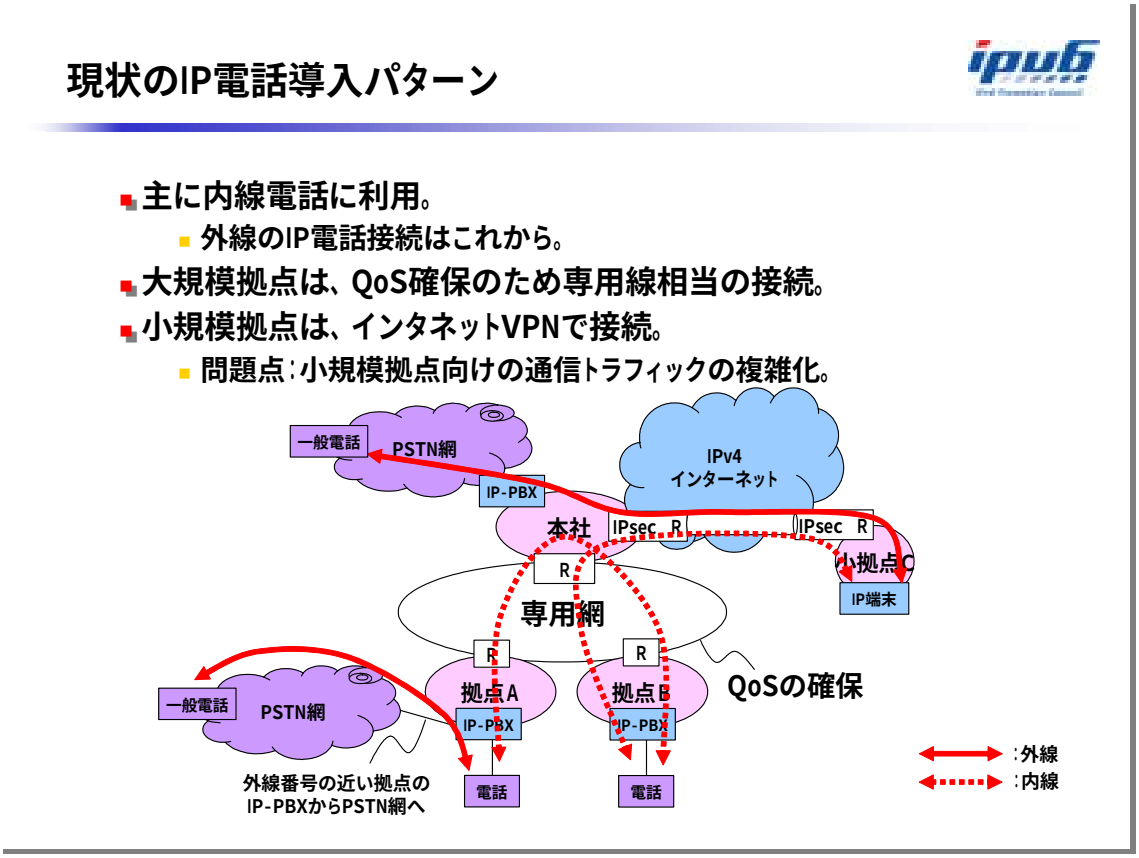
(3) VoIPv6 ソリューション

IP 電話の外部接続に関するコストを削減するソリューションで、IPv6 契約をし、必要なトラフィック用にファイアウォールに穴を開けるだけで利用できます。これから広まると考えられる IPv6 電話の外部接続は、IPv4 電話の外部接続と比較してコストを削減できます。

その理由は、外線ゲートウェイ（SIP-NAT）装置の負荷軽減、グローバルアドレス取得のコスト軽減、IP 電話トラフィックの単純化（センタ集中を回避）にあります。

当面、ファイアウォールで IPv6 電話に関するトラフィック（プロトコル ID やアドレス指定）のみの通過を許可することで、セキュリティを確保できます。実際の導入に際しては、各企業のセキュリティポリシーにより、独立融合型，段階置換型を選択します。

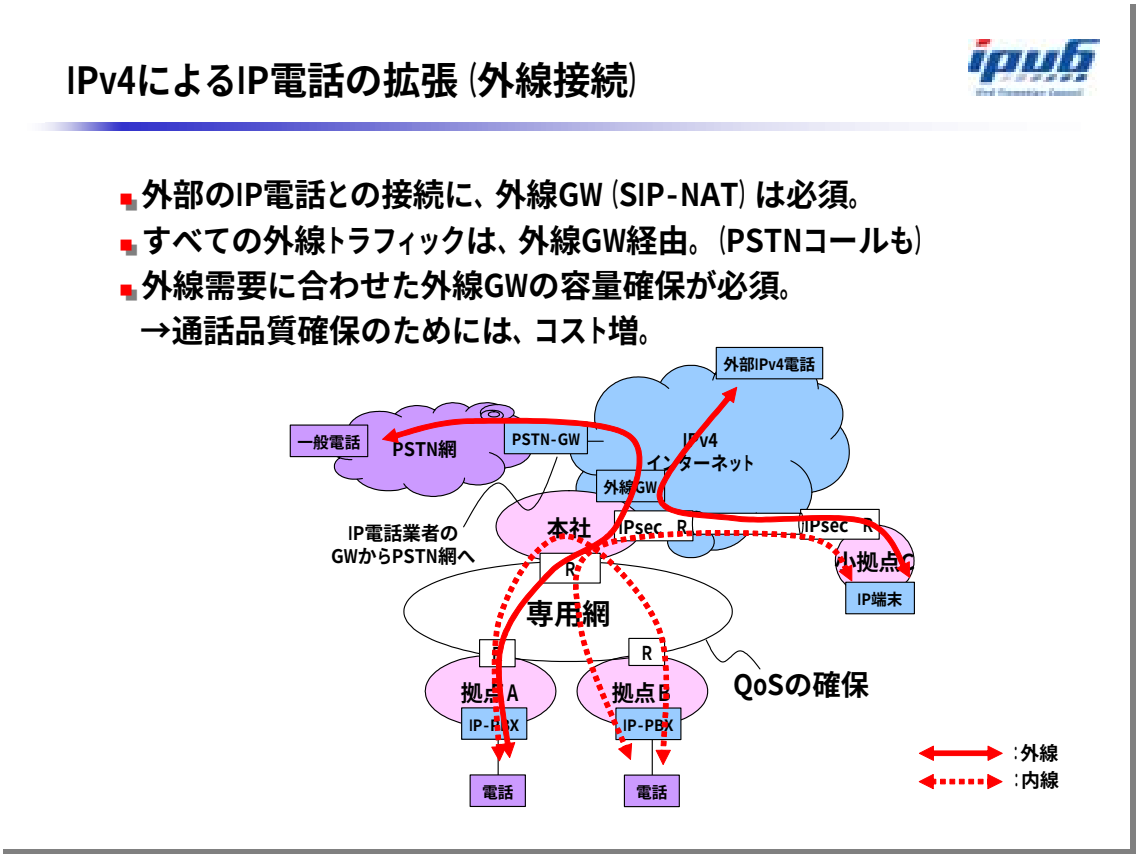
(3) 現状の IP 電話導入パターン



IP 電話に限らず、何かのアプリケーションについて、ゲートウェイの負荷がネックなる場合に、IPv6 を使い「○○ソリューション」として同じ論理で構築が可能です。

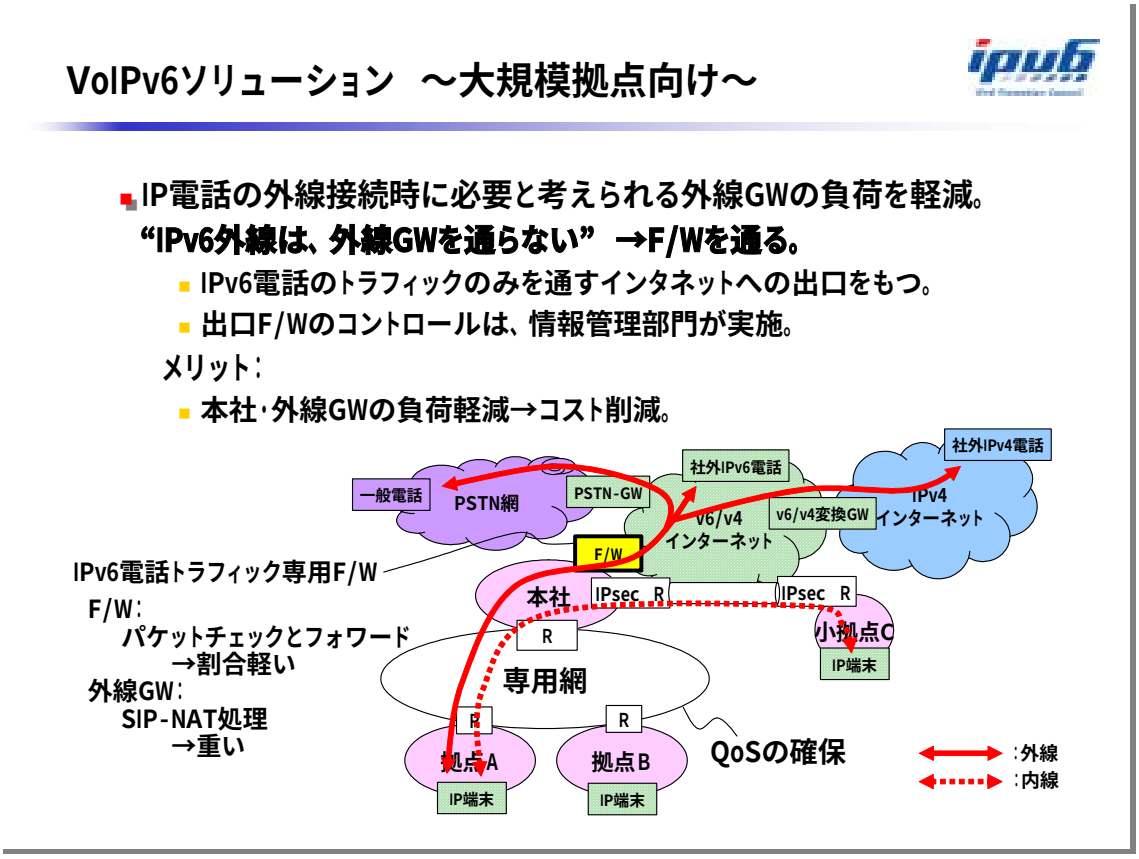
IP 電話は、現在主に内線電話に利用されており、外線の IP 電話接続はこれからです。IPv4 ソリューションでは、大規模拠点は QoS 確保のため専用線相当の接続を行い、小規模拠点はインターネット VPN で接続されます。しかし、小規模拠点向けの通話トラフィックの経路が複雑になってきます。

(4) IPv4 による IP 電話の拡張（外線接続）



IPv4 による IP 電話では、外部の IP 電話との接続に、外線ゲートウェイ（SIP-NAT）は必須です。すべての外線トラフィックは、外線ゲートウェイ経由となります（PSTN コールも）。外線需要に合わせた外線ゲートウェイの容量確保が欠かせません。したがって通話品質確保がコスト増につながります。

(5) VoIPv6 ソリューション　～大規模拠点向け～



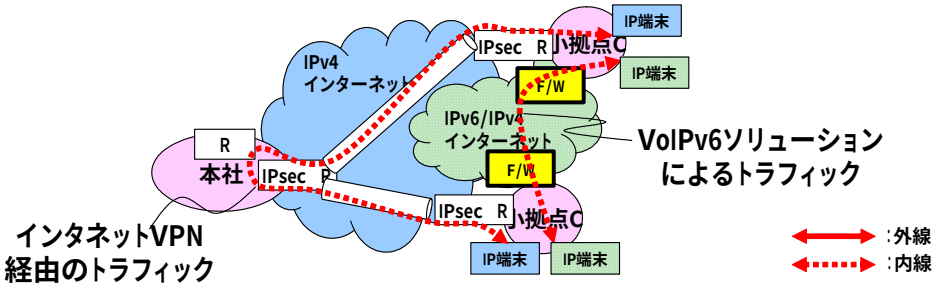
大規模企業において VoIPv6 ソリューションを導入することで、IP 電話の外線接続時に必要と考えられる外線ゲートウェイの負荷を軽減することができます。IPv6 外線は、外線ゲートウェイを通らず、ファイアウォールを通ることになるからです。この場合、IPv6 電話のトラフィックのみを通すインターネットへの出口を設定することになります。(出口のファイアウォールのコントロールは、情報管理部門が実施します。)

これにより、本社の外線ゲートウェイにおける負荷が軽減されることで、コスト削減が可能になります。

(6) VoIPv6 ソリューション　～小規模拠点向け～

VoIPv6ソリューション　～小規模拠点向け～

- 小規模拠点での、インタネットVPN経由のトラフィックを単純化。
  拠点F/W：
  - IPv6電話のトラフィックのみを通すインタネットへの出口をもつ。
  - 出口F/Wのコントロールは、情報管理部門が実施。
  メリット：
  - 新たなIPv4アドレス不要→コスト削減。
    (IPv4で同じ構成をとる場合、新たなグローバルアドレスが必要)
  - インタネットVPN経由の通話トラフィックの単純化。



また、小規模拠点における VoIPv6 の導入は、小規模拠点でのインターネット VPN 経由のトラフィック経路の単純化につながります。

この場合、各拠点のファイアウォールが、IPv6 電話のトラフィックのみを通すインターネットへの出口を持つことになります。(出口ファイアウォールのコントロールは、情報管理部門が実施します。)メリットとしては、新たな IPv4 アドレスを入手する必要がなくなるため、コスト削減につながります(IPv4 で同じ構成をとる場合、新たなグローバルアドレスが必要)。また、インターネット VPN 経由の通話トラフィックの経路を単純化することができます。

(7) VoIPv6 ソリューション　～もう１つのメリット～

VoIPv6 の実現によるメリットはまだあります。

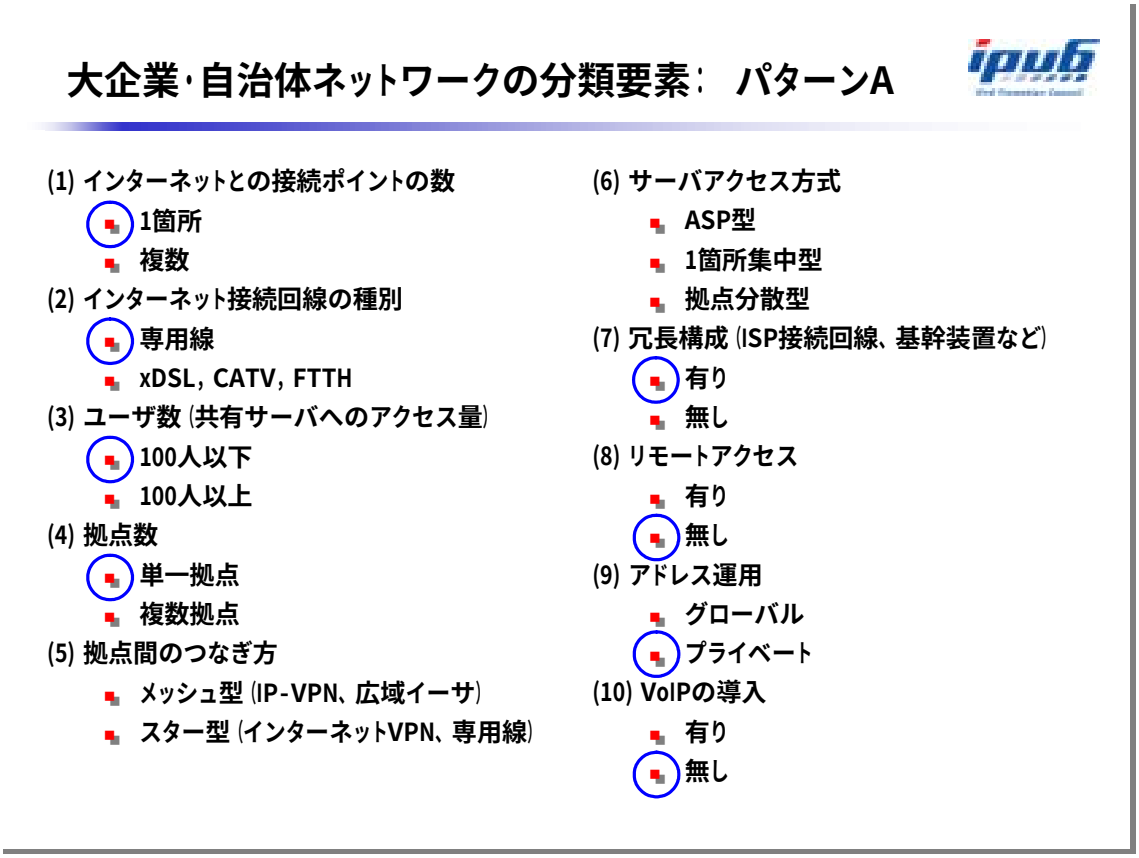
IP 内線電話機が普及するとアドレスが 2 倍近く必要となります。たとえば 100 人の職場で、サーバ、ルータ、プリンタ、無線アプリケーション用（固定割り当て）に 50 個、PC 用（DHCP 割り当て)に 150 個（合計 200 個＝/24 で運用可能）必要となっているとしましょう。そこでさらに IP 内線電話機を 120 台追加すると、合計 320 個のアドレスが必要となります。この数は、/24 ではオーバフローしてしまいます。したがって、IPv4 の場合は、サブネットマスクの変更や、別セグメントの追加（＝IP 電話機を別セグメントとして定義）など、サブネットの再設計が必要となり、結果として再設計のコストが大きくなります。しかし、IPv6 ならば、IPv4 で必要とされる再設計（端末数増加によるサブネットの再設計等）は不要です。

■具体的な IPv6 導入イメージ

以下では、**大企業・自治体**組織の構成から A と B の 2 つのパターンを想定し、それぞれについて現状で実現可能な IPv6 への移行方法について紹介します。

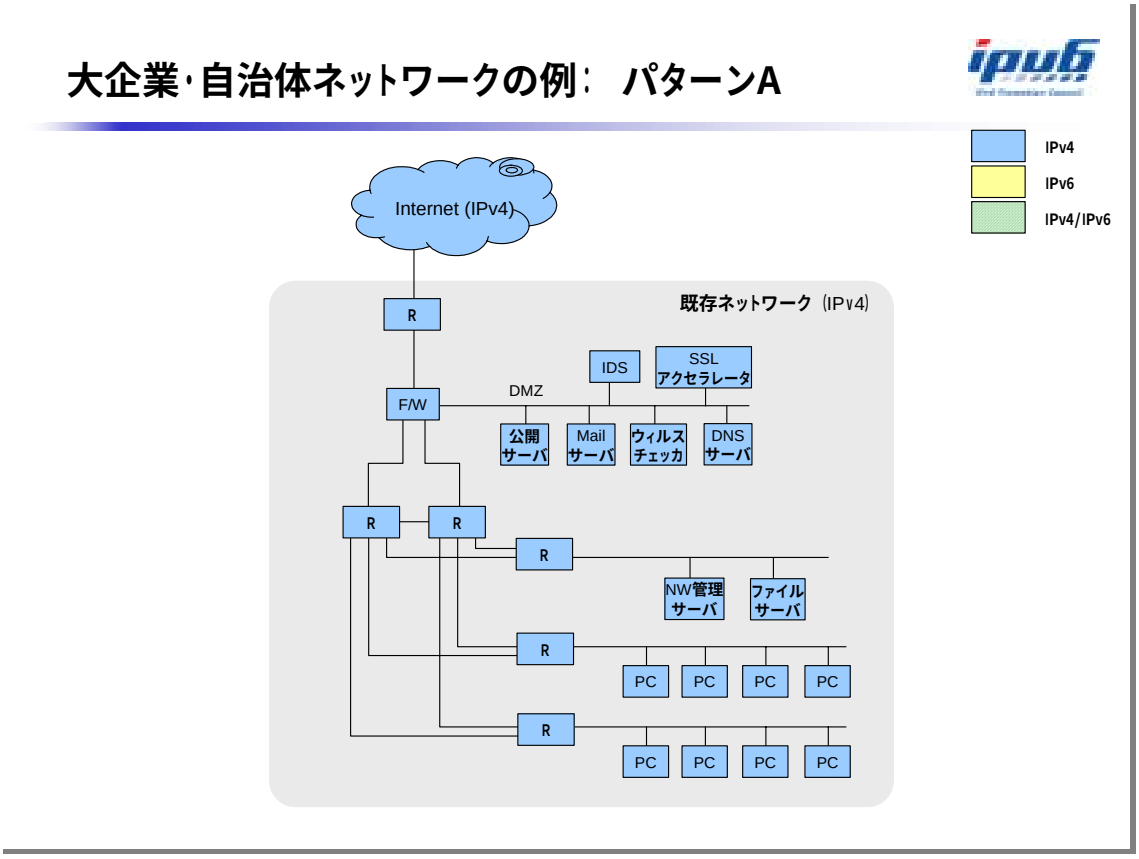
(1) パターン A

ネットワークの分類要素



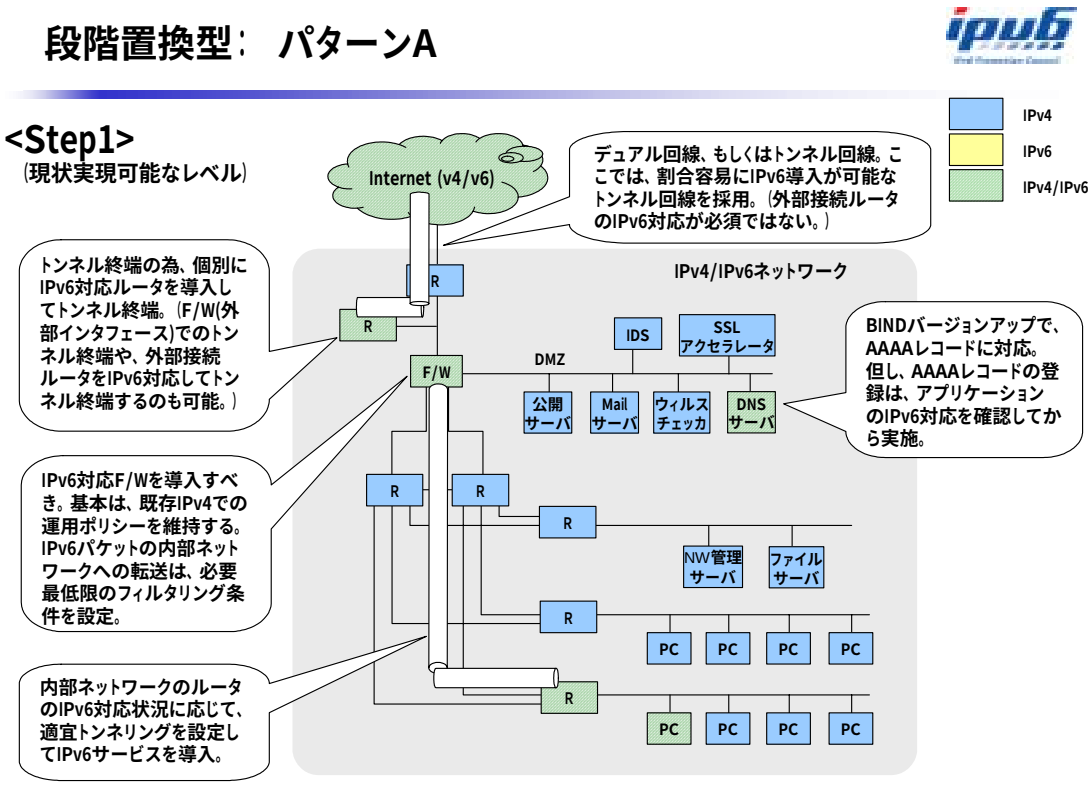
パターン A は、比較的小規模でシンプルなネットワークです。拠点は 1 ヵ所しかなく、ユーザ数も 100 人以下です。インターネットとは専用線で接続されていて、リモートアクセスは提供していません、VoIP も導入していません。

ネットワークの例



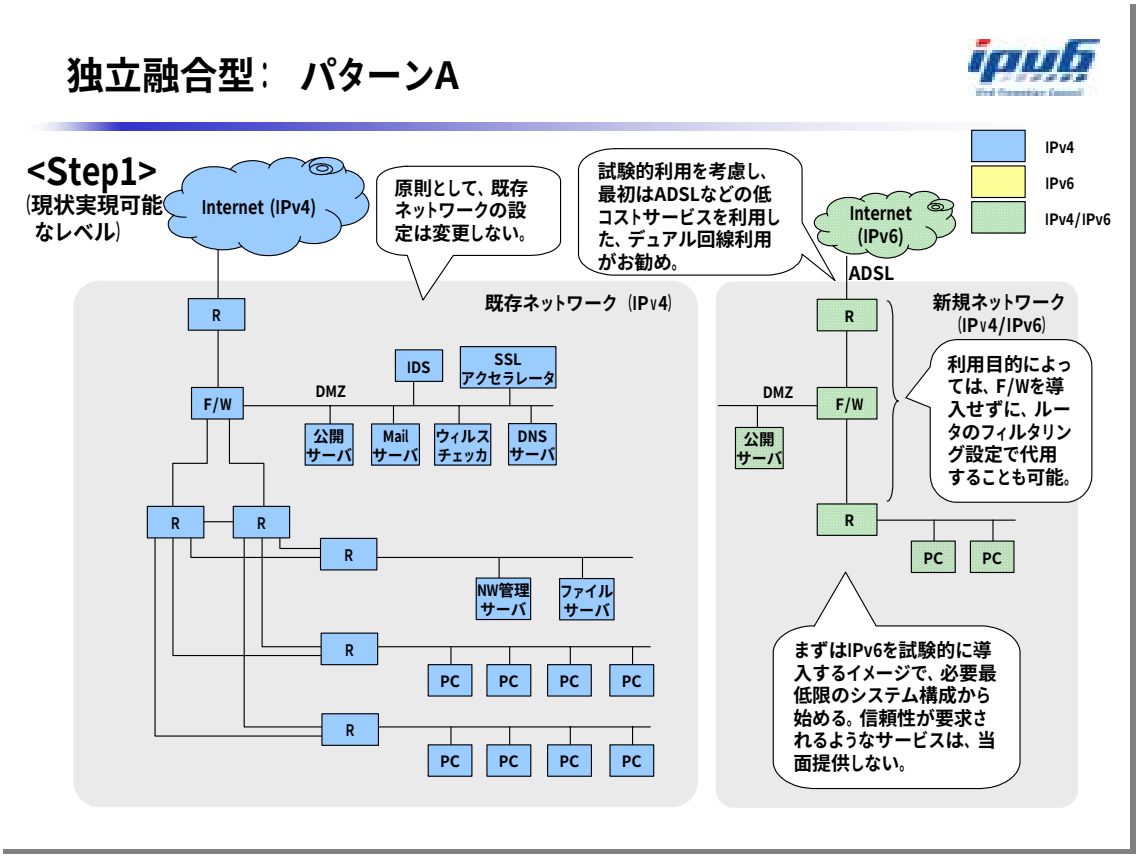
インターネットとの接続は 1 ヵ所です。図に示したように、Web サーバやメールサーバ、DNS サーバを DMZ に配置しています。

段階置換型の移行



まず、段階置換型の移行については、上の図のような形態が考えられます。IPv6 接続はデュアルあるいはトンネル回線ですが、ここでは導入の容易さからトンネル回線を選択しています。IPv6 対応ルータを別個に導入して、トンネルの終端用を行っています。また、IPv6 対応ファイアウォールを導入して、IPv4 相当のポリシーを維持します。

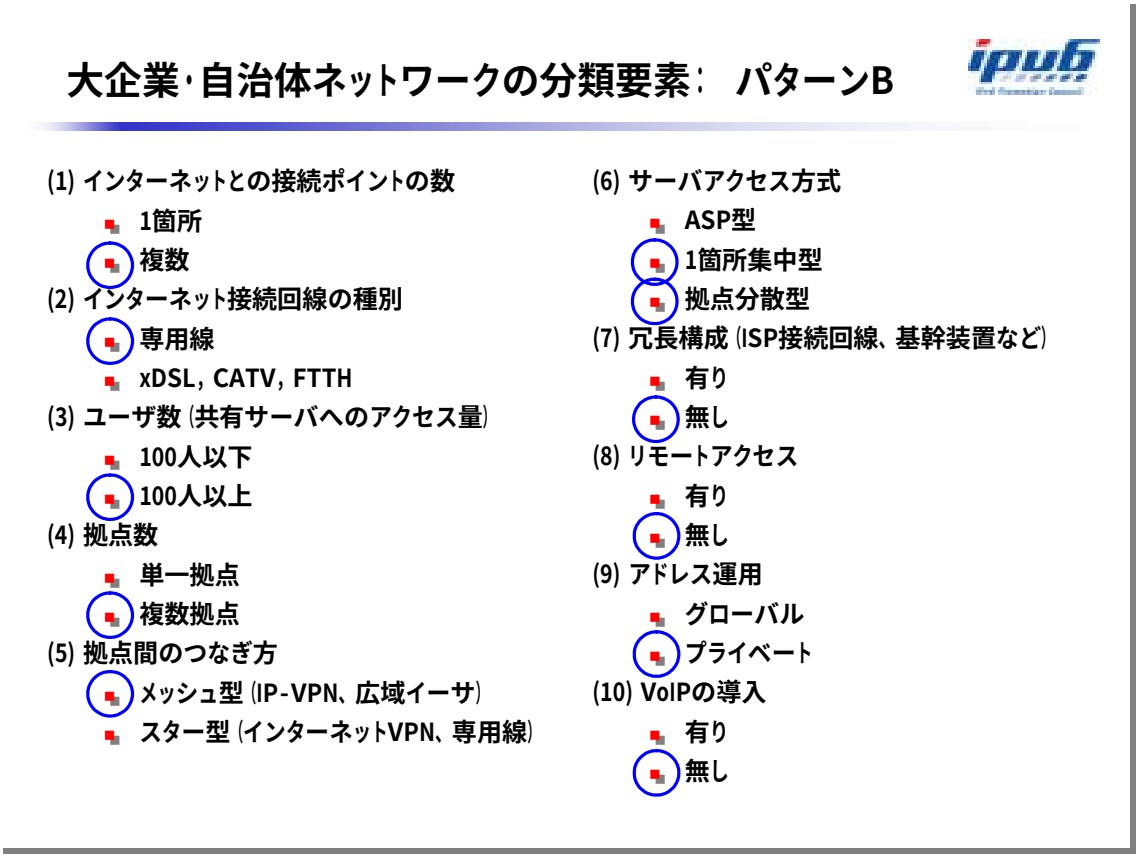
独立融合型の移行



独立融合型の移行では、原則として既存ネットワークにはまったく変更を加えず、別個に IPv6 接続を持ったネットワークを構築します。この IPv6 ネットワークでは、まずは IPv6 を試験的に導入するイメージで、必要最低限のシステム構成から始めるのが望ましいと思われます。したがって、利用目的によっては、ファイアウォールを導入せずに、ルータのフィルタリング設定で代用することも可能です。

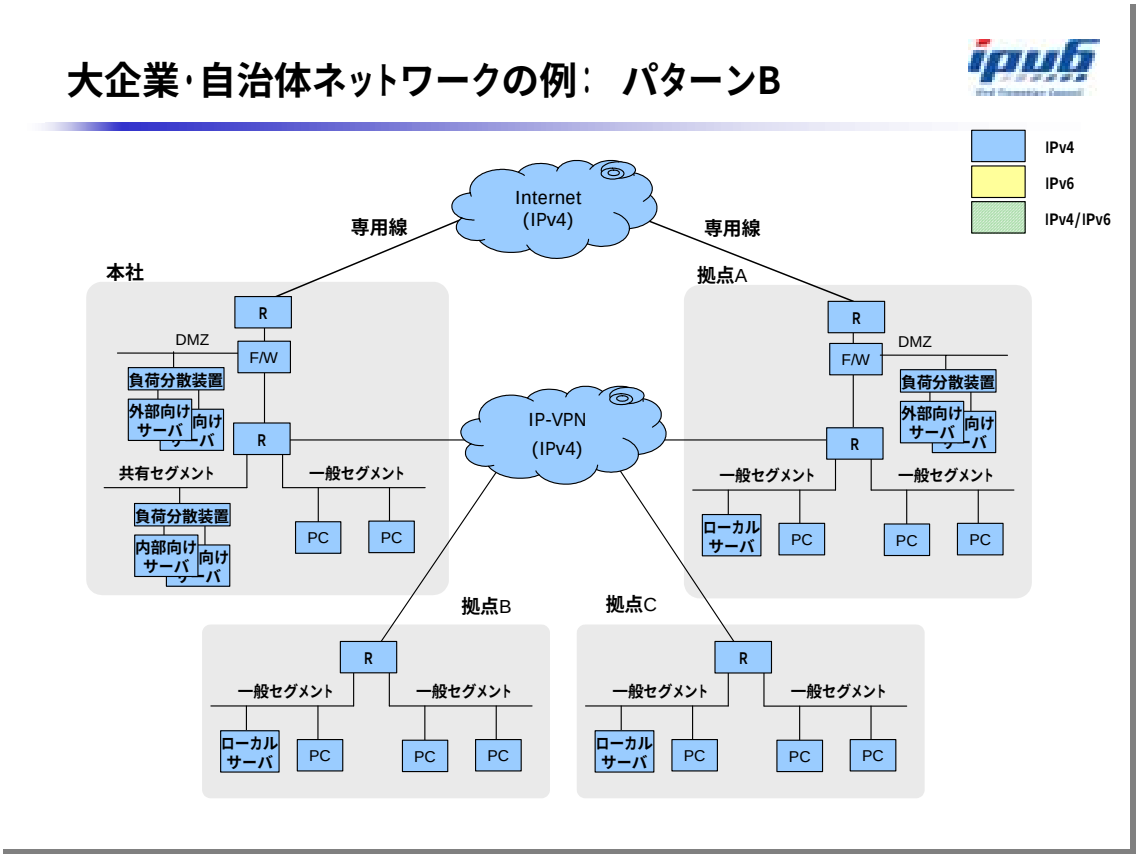
(2) パターン B

大企業・自治体ネットワークの分類要素



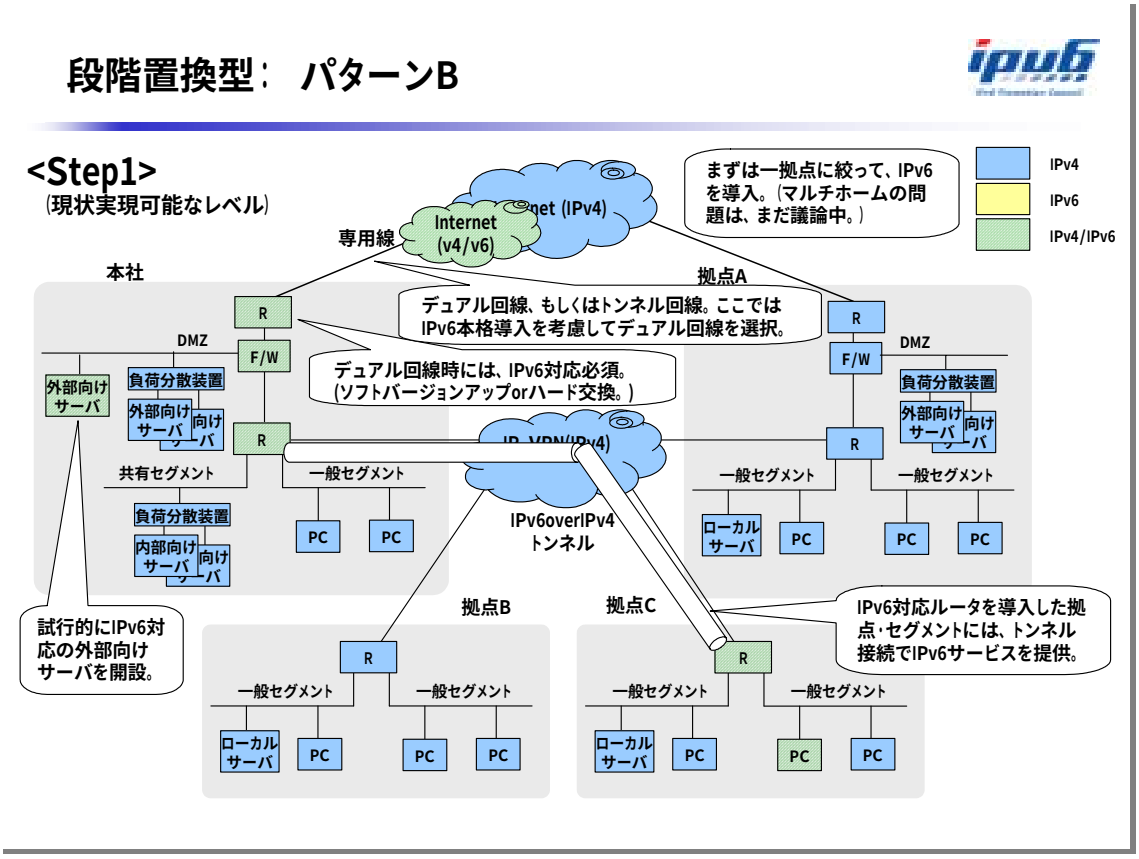
パターン B は、たとえば 100 人以上のユーザを持ち、複数の接続ポイントでインターネットとつながっているような、より大規模な企業や自治体を想定しています。

ネットワークの例



拠点間はメッシュ型の接続となっています。

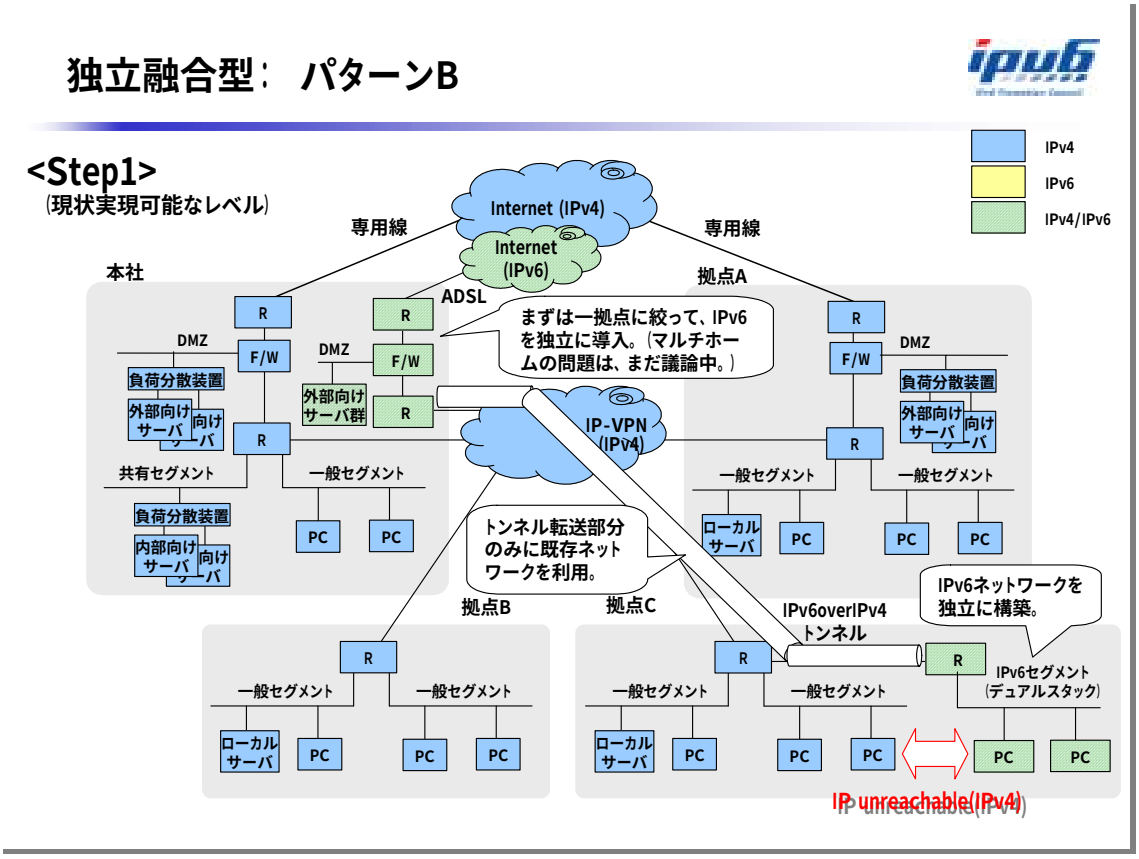
段階置換型の場合



パターン B における段階置換型の移行については、図のような形態が考えられます。IPv6 接続はデュアルまたはトンネル回線ですが、この図では将来的な本格導入を見据えて本社にデュアル回線を選択しています。デュアル回線を選択した場合は、外部との接続ルータが IPv6 対応をする必要があります。ここでは外部との IPv6 接続を 1 回線に限定しています。その理由の 1 つは、IPv6 におけるマルチホーミングに関する議論がまだ決着していないことにあります。

また、ここでは本社以外にも、IPv6 over IPv4 トンネリングにより一部の拠点に IPv6 接続を提供しています。

独立融合型の場合



独立融合型の移行については、上の図に見られるとおり、既存ネットワークと完全に切り離された形で IPv6 ネットワークを構築しています。ここでは別拠点に対しても IPv6 over IPv4 トンネリングによって IPv6 接続を延長していますが、延長先においても IPv4 と IPv6 のネットワークは完全に独立しています。

3. 5:5 段階に向けて

■5:5 段階において想定される IPv6 利用環境と基本方針

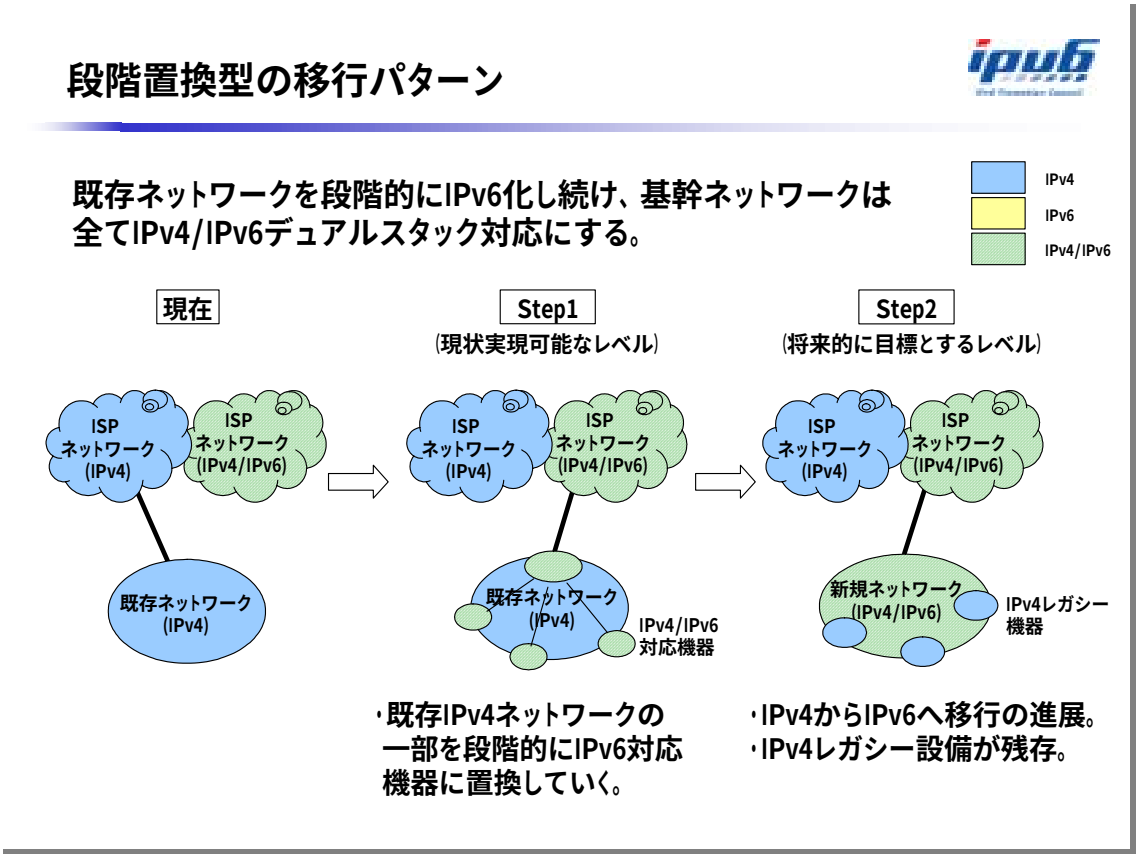
IPv4 対 IPv6 が 5 対 5 の世界では、IPv6 ネットワーク環境が現在よりも大幅に充実していることが想定されます。まず、中小規模 ISP による IPv6 回線サービス（デュアルスタック、トンネル）も始まり、ルータでは大型から小型まで、IPv6 対応製品のバリエーションが充実します。また、基本 OS では、モバイルや IPsec をはじめとした IPv6 機能への本格対応が見られるようになります。また、各種 IPv6 対応アプリケーションソフトが普及します。ファイアウォール、IDS などのセキュリティ対策製品で、IPv6 対応製品が充実します。

また、この時期になると、ネットワークが従来の枠組みを超えて広がっていきます。まず、nonPC 機器のネットワーク接続が進み、ユビキタス化の進展が見られるようになります。また、組織単位のセキュリティ管理から個人単位のセキュリティ管理へ、人々の認識もシフトしていくでしょう。経験の蓄積により、IPv4/IPv6 デュアル環境でのセキュリティポリシーが確立することも期待できます。そして新しいセキュリティポリシーの元で、 IPv6 の特徴・メリットを生かしたアプリケーションが普及し始めることになり、IPv4 から IPv6 中心のネットワーク利用形態へ、移行が加速するでしょう。その一方で、IPv6 を使った侵入や攻撃、その他の不正行為が本格化していくでしょう。

この時期の基本方針としては、組織全体として IPv4/IPv6 のデュアルスタックネットワーク環境に移行すべきです。旧来のアプリケーションは無理に IPv6 へ対応させる必要はありませんが、全体的には順次 IPv6 中心のアプリケーション利用環境へシフトしていくべきです。

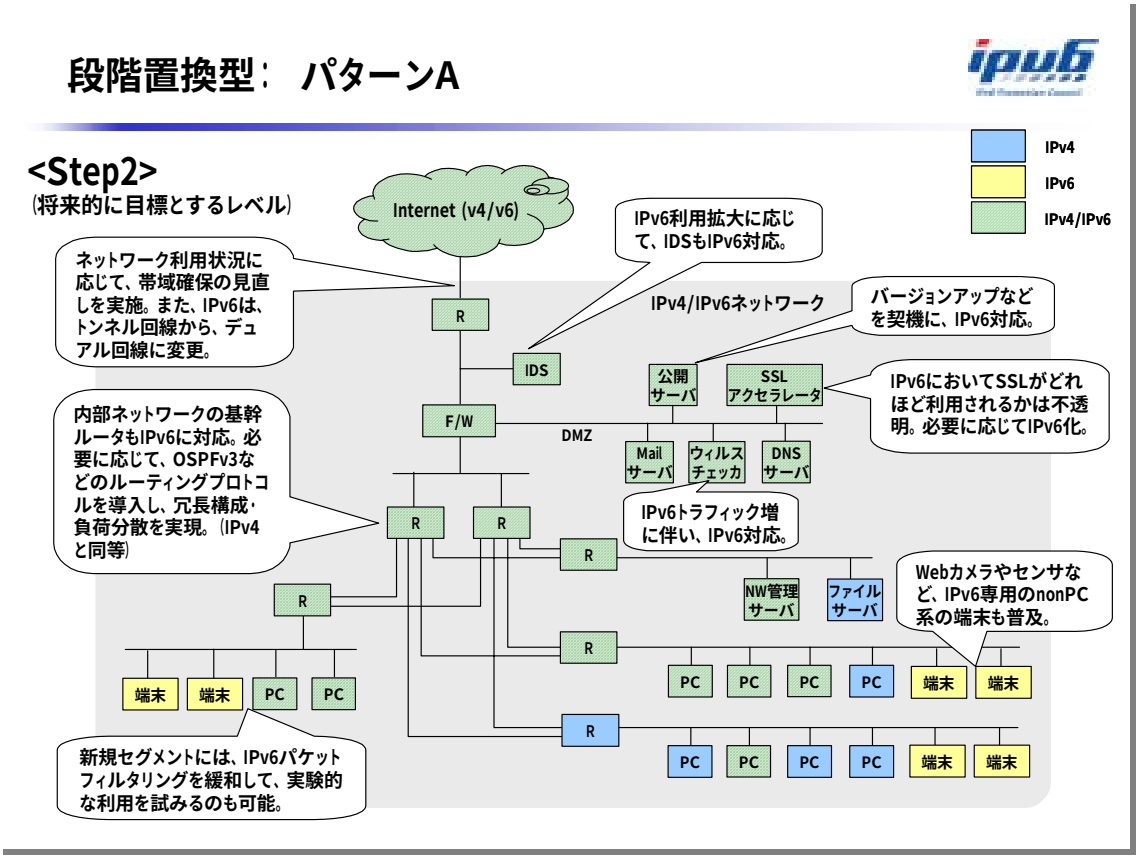
■段階置換型の場合

(1) 移行パターン



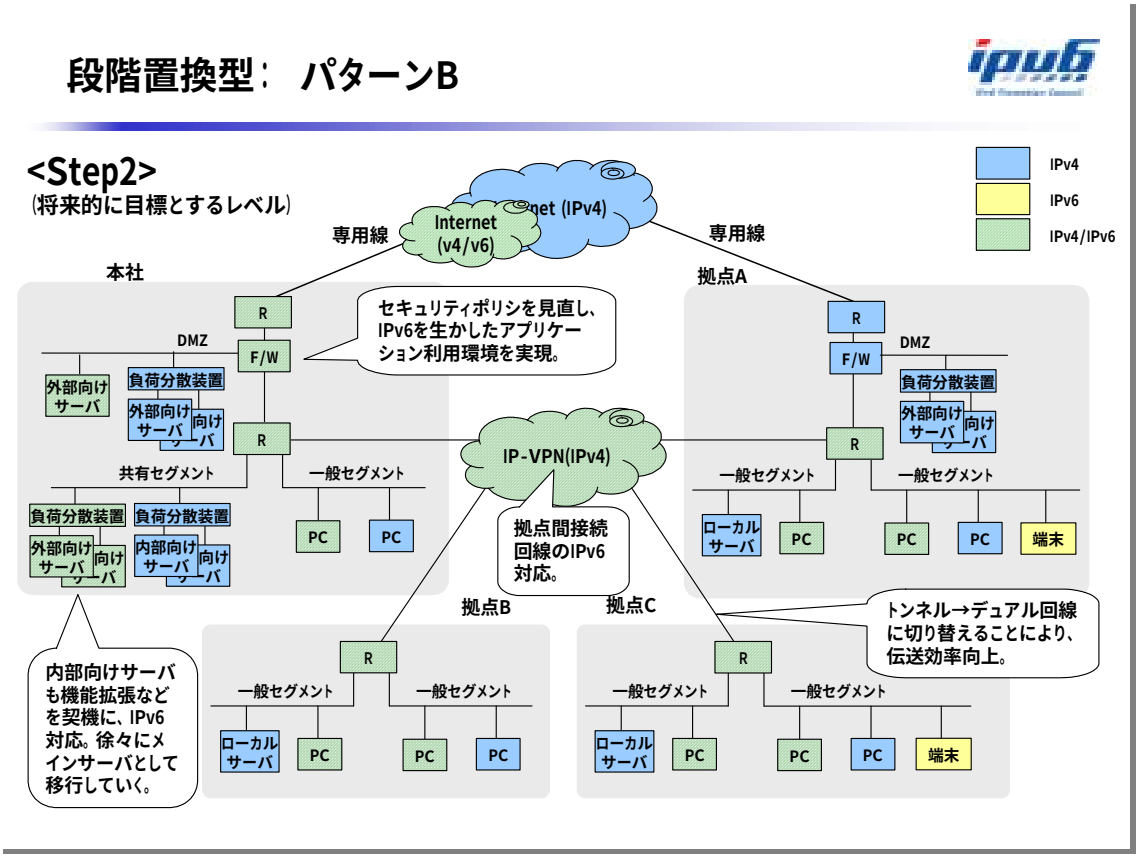
段階置換型の大まかな移行イメージは図のようになります。まず現状で実現可能なレベルとして、既存 IPv4 ネットワークの一部を IPv4/IPv6 のデュアルスタックとし、次のステップとして将来的には、IPv4/IPv6 のデュアルスタック端末を基本とし、一部の従来からの端末のみ IPv4 オンリーで使い続けます。

(2) パターン A



このような状況を前提として、パターン A の企業や自治体が将来的に目標とするネットワークは、段階置換型の場合、図のようなものとなります。ここでは、内部の端末のほとんどがデュアルスタックとなり、IPv6 も話すようになっている様子を示しています。インターネット接続回線は、トンネルからデュアルに変更します。また、ネットワークニーズの見直しで、必要通信帯域を確保します。基幹ルータも IPv6 対応の製品に入れ替えます。OSPFv3 などのルーティングプロトコルを導入し、IPv4 と同等の冗長構成・負荷分散を実現します。ウィルスチェッカや IDS については、IPv6 トラフィックの増加にともなって IPv6 対応の製品を導入していきます。公開 Web サーバ用の SSL アクセラレータについては、IPv6 時代にどれくらい使われるかが未知数です。これについては必要に応じて IPv6 対応がなされることになります。

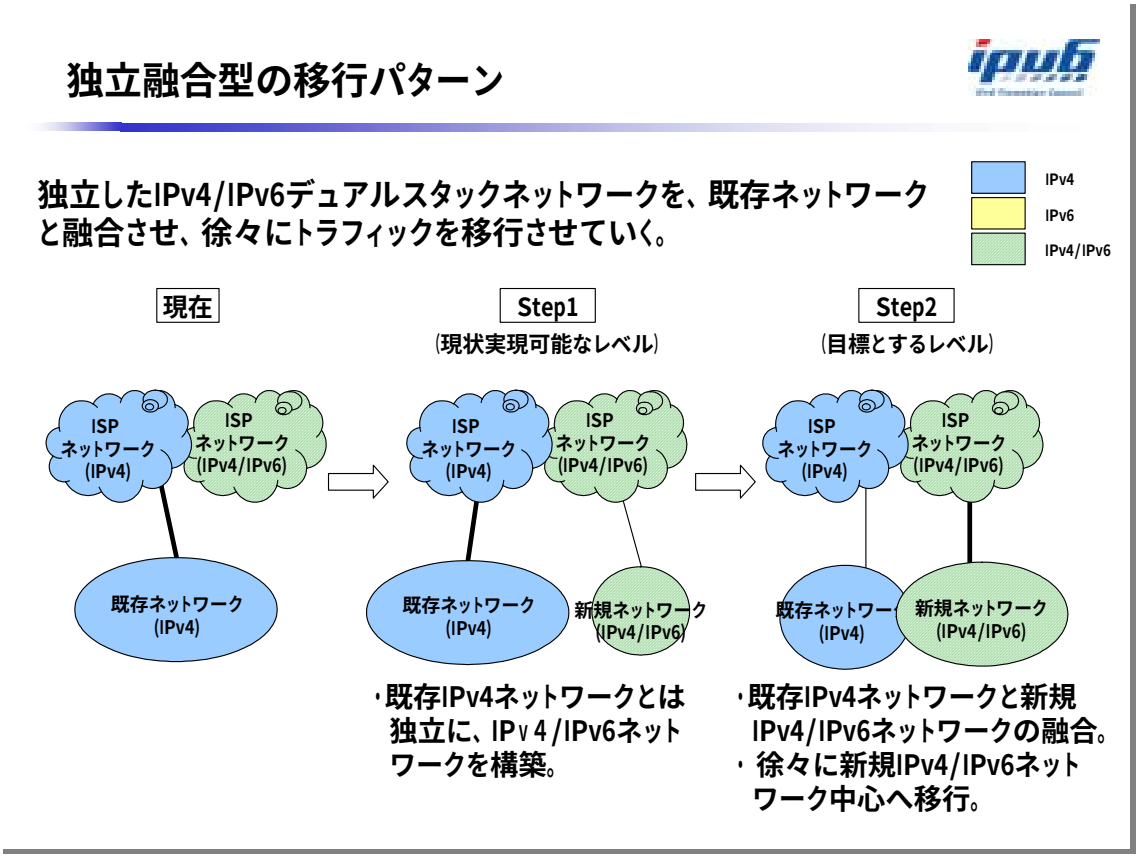
(3) パターン B



パターン B の企業や自治体の段階置換型移行でも、5 対 5 の環境で目指すネットワークにおいては、社内における各拠点の端末の大多数が IPv4 と IPv6 の双方で通信できる状態になっています。外向けのサーバに続き、内部向けのサーバについても、機能拡張やバージョンアップを機に、デュアルスタック化を実現します。拠点間接続も IPv6 対応します。

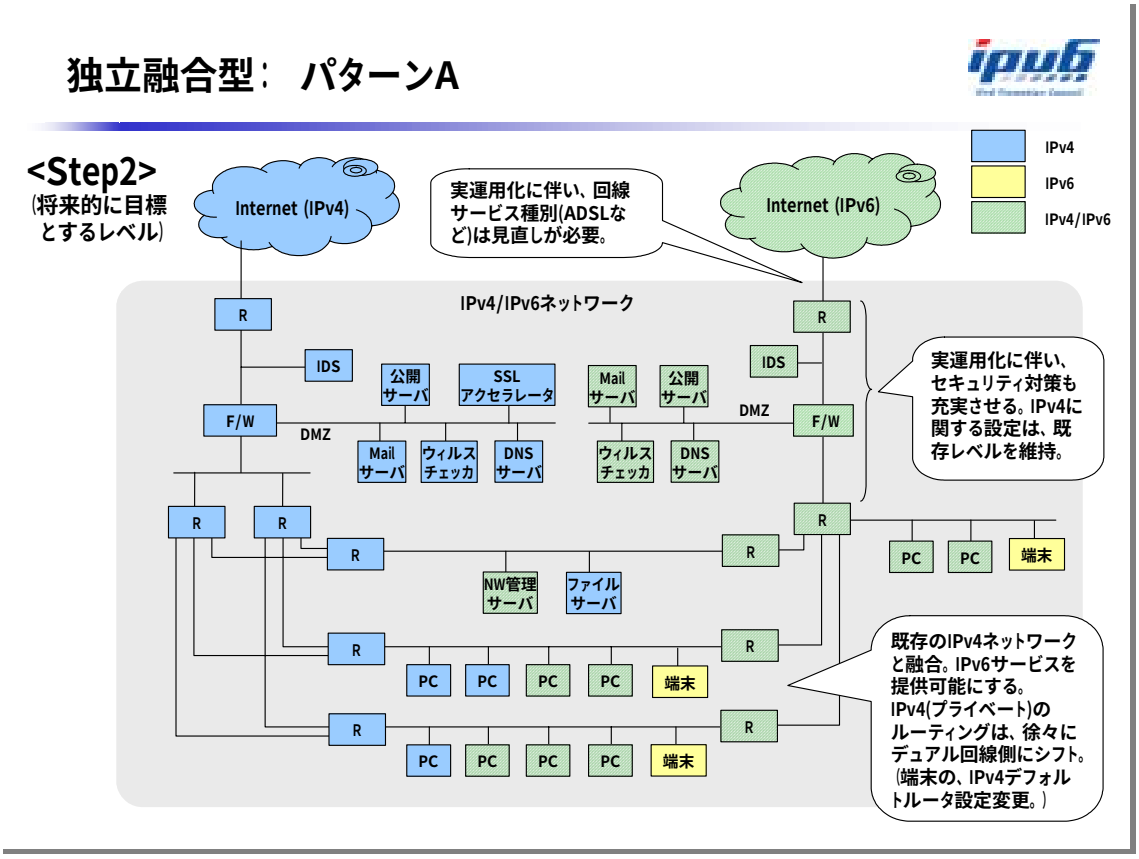
■独立融合型の場合

(1) 移行パターン



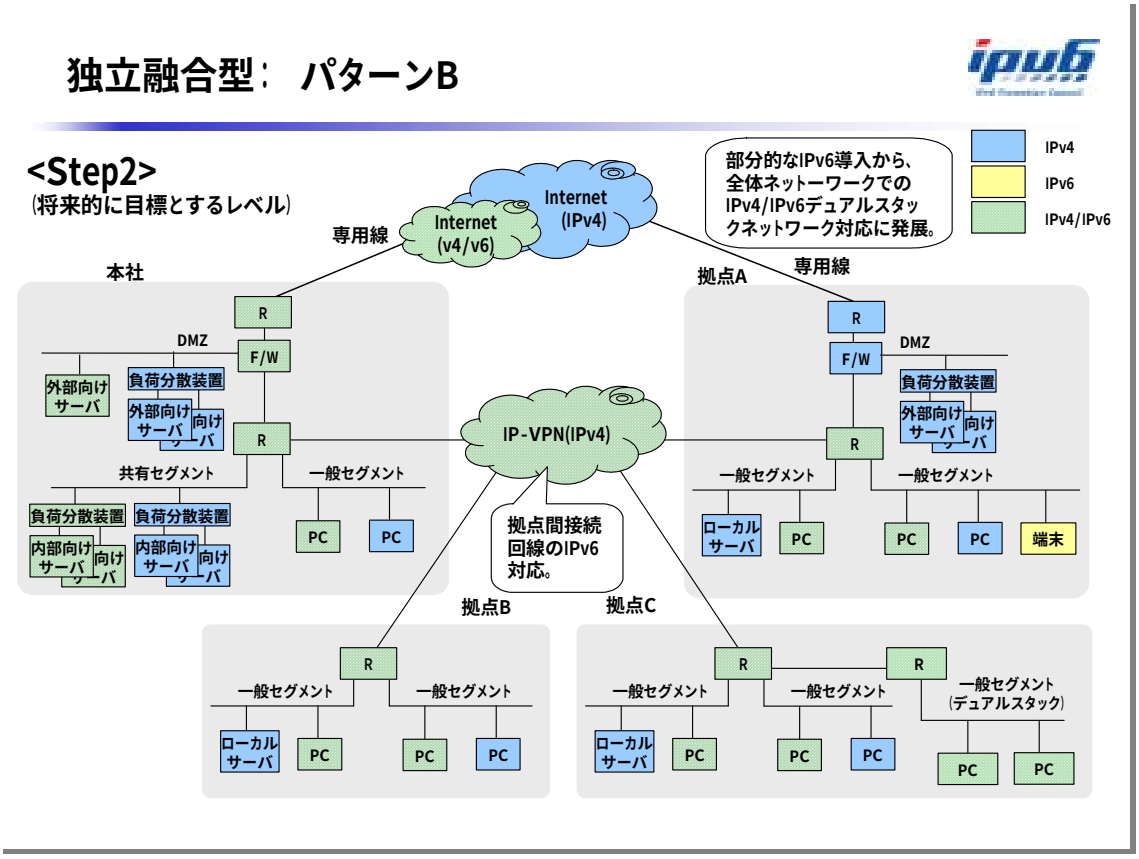
独立融合型では、まず現状実現可能なレベルとして、既存の IPv4 ネットワークについてはそのままとし、別個に IPv4/IPv6 ネットワークを構築します。そして将来目標とするレベルとしては、既存 IPv4 ネットワークと新規 IPv4/IPv6 ネットワークを融合させ、徐々に新規 IPv4/IPv6 ネットワーク中心へ移行します。

(2) パターン A



独立融合型の移行形態をとる場合、パターン A の企業や自治体では、これまで完全に独立して構築されてきた IPv4/IPv6 デュアルネットワークを、既存の IPv4 ネットワークと融合します。その上で、既存ネットワークにおける IPv4 ルーティングは、徐々にデュアル回線側に切り替えていきます（端末の IPv4 デフォルトルータ設定を変更する）。IPv4 ネットワークとの融合に伴い、デュアル回線側のインターネット接続点におけるセキュリティ設定は、IPv4 のレベルを維持するものにします。

(3) パターン B



パターン B の企業や自治体においても、既存ネットワークとの融合により、全体的にデュアルスタックネットワークへと発展させます。

■IPv6 で実現したいネットワーク環境

理想的なネットワーク環境

大企業や自治体における理想的なネットワーク環境の条件は、プラグ・アンド・プレイが可能であり、かつ安全性と管理性に優れていることです。

エンドユーザは、端末をつなげば設定なしに適切な相手とだけ安全に通信できるのが理想的です。一方、管理者は、容易に端末の所有者/場所を同定でき、エンドユーザの設定を一括管理できるような環境が望まれます。

ネットワークトポロジー

IPv4 の環境から特に変更されることはないと考えられますが、MobileIPv6、もしくはそれ相当の技術の実用化に伴い、接続端末の場所は自由に移動できるようになるでしょう。

プロトコルスタック

デュアルスタックが基本となります。IPv6 オンリーの端末もそのうち出てくることが考えられますが、各種サーバをデュアルスタックにするか IPv6 オンリーにするかの選択は、IPv4 と IPv6 の 2 つのスタックを運用することのコストと、アプリケーションの IPv6 化のコストとの間のトレードオフ的関係のバランスによって決まります。

セキュリティ

セキュリティについては、エンドツーエンドの通信を全端末に許すか、特定の端末にだけ許すかに関する判断が求められます。特に外部との間のエンドツーエンドの暗号化を可能にするかどうかが問題となります。これは、管理者が任意の通信をチェックできるかどうかという問題と関わってきます。

IPv6 らしさの実現

大企業や自治体において、「IPv6 らしさ」を生かそうとする際には、モビリティの活用がトピックとして浮上します。また動的な名前登録（ダイナミック DNS や SIP の利用が考えられます）や Mobile IPv6 の利用に期待が持てます。IPv6 らしいもう 1 つの利用方法はエンドツーエンド通信です。SIP に基づく VoIP（内線、外線）、テレビ会議、ファイル共有、インスタントメッセンジャーなどがこれにあたります。

他の端末からのアクセス制御法

エンドツーエンド通信が実現可能なネットワーク環境下では、各端末に対する他の端末からのアクセス制御方法を新たに考えることになります。パーソナルファイアウォールの利活用方法については、今後十分な検討が必要になるでしょう。一般社員による外部からのアクセスにおいては、IPsec やファイアウォールをどのように機能させるかが重要なポイントになります。

また、機器メンテナンスのための外部からのアクセスについては、インターネット接続回線を利用するのか、別回線にするのかといった点も考慮する必要があるでしょう。内部アクセスのセキュリティについては、ソーススプーフィング攻撃対策、端末直収ルータによるフィルタリング、レイヤ 2 スイッチによる異常 RA のフィルタリング、ランダムなアドレスで

通信ができるプライバシーエクステンションに関する対策などを検討するべきです。

全般的には、組織ネットワーク内のネットワークサービスとしてどこまで何を認め、ネットワーク管理としてどこまで何を管理するべきかという問題を、組織毎に整理する必要があります。

4. 5:5 に向かうための課題

■マルチホーム

マルチホーム

＜マルチホームのメリット＞

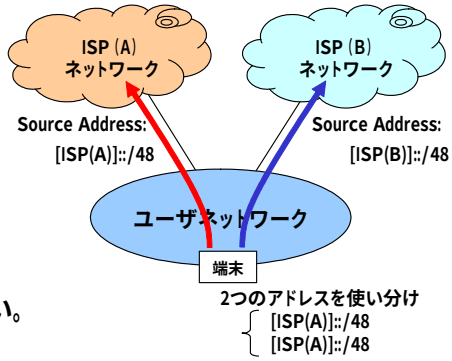
- インターネットへの接続に冗長性が確保される。
- 経路最適化や負荷分散が設定可能。

→IPv4ネットワークでは、多くのユーザが何とか適用できていた。

＜IPv6のアドレスポリシー＞

- ルーティングの経路集約を重視する為、階層（ツリー）構造のアドレス管理。
- 全ての一般ユーザは、一意のISPからアドレスを取得。

→原則として、2通り以上の経路は発生しない。



＜問題点＞

- 各端末にマルチプレフィクスを割当て、Source Address Selectionで対応。
  →端末に知的なアドレス選択アルゴリズムが必要。
  →ISP回線障害時の処理が困難。
- ISP側にパンチングホールを設定。
  →経路情報の増大。

マルチホームは、大企業や自治体のネットワークにとって大きなメリットをもたらします。インターネットへの接続に冗長性が確保されるほか、経路最適化や負荷分散を実現することができるからです。

IPv4 ネットワークでは、多くのユーザが何とかマルチホームを実現していました。しかし IPv6 では、原則として単一の一般ユーザネットワークに対して 2 通り以上の経路が発生しないことになっています。IPv6 のアドレスポリシーとして、ルーティングの経路集約を重視するため、階層（ツリー）構造のアドレス管理をしており、すべての一般ユーザは、接続性の提供を受ける ISP からアドレスを取得する決まりになっているからです。

しかし、IPv6 では、各端末に複数のネットワークプレフィックスを持つアドレスを割り当て、送信アドレスを用途に応じて使い分けることができます。これを Source Address Selection と言います。ただし、端末に知的なアドレス選択アルゴリズムが必要となります。また、ISP 回線障害時の処理が困難です。

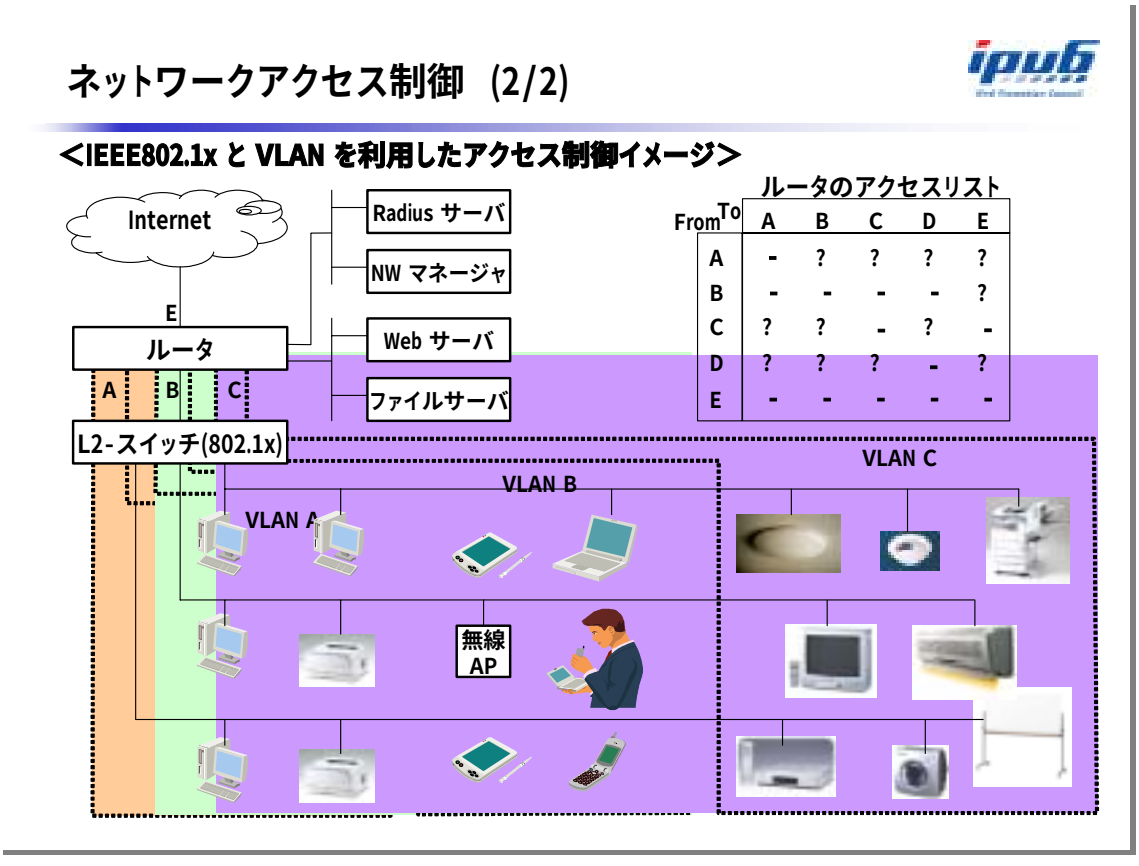
もう 1 つの方法は、ISP 側にパンチングホールを設定することですが、この場合、経路情報が増大します。

マルチホームについては、IPv6 を実用的に利用するために解決しなければならない大きな課題の 1 つといえます。

■ネットワークアクセス制御

IPv6 ネットワークでは、多種多様な機器がネットワーク接続されていくことが想定されます。従業員の PC、プリンタ、従業員以外の PC や PDA、その他ホワイトボード、複写機、照明、空調、センサ、監視カメラ、TV などです。しかし、これらの機器を同一レベルで管理する必要はありません。このため機器毎に異なるレベルのネットワークアクセス制御を設定したいところです。

解決策としては、VLAN を使用してネットワークをいくつかのセグメントに分割し、IEEE802.1x 認証を利用して、機器を適当なセグメントに接続させることが考えられます。セグメント毎にアクセス制限を設け、たとえばあるセグメントに対しては、従業員の PC のみを接続させてすべてのアクセスを許可、またあるセグメントに対しては、その他の PC を接続させて制限されたアクセスのみを許可（“guest” アカウント利用など）、そしてその他のセグメントにその他の機器を接続させて内部アクセスのみ許可する、といったポリシーを適用することができます。



現在、無線 LAN におけるユーザ認証で広がりつつある 802.1x は、もともと有線のネットワークを対象としたものですが、その認証情報に基づいて異なる VLAN に割り当てる仕組みを使えば、PC や各種の非 PC 機器を、目的や用途に応じて別個のセキュリティ空間に属させることができます。

■その他の 5:5 に向かうための課題（セキュリティ関連除く）

その他の課題としては、ISP との回線接続契約を IPv4 から IPv4/IPv6 デュアルスタックへ切り替える時や、主要な外部接続回線を既存ネットワーク回線から、新規ネットワーク回線へ切り替える時にアドレスのリナンバリングが発生します。変更のための工数を最小化するための方策が望まれます。

また、インターネットサービス基盤として、ISP だけでなく IDC やホールセラーなどの IPv6 対応も求められます。

各種アプリケーション関連では、以下のような点を解決する必要があります。

DNS

DNS ディスカバリ、DNS 登録手法、新たなネーミング手法。

メール・Web

ウィルスチェッカ・コンテンツチェッカの IPv6 対応。

グループウェア

専用クライアントソフトウェアの対応（Web サービス化含む）、サーバの IPv6 化技術の利用（リバースプロキシ、トランスレータなど）。

ファイル共有

ネーミング、シグナリング、セキュリティ確保。

マーケットプレイス

各種専用ソフトの対応。

5. セキュリティモデル

■セキュリティに関する基本的な考え方

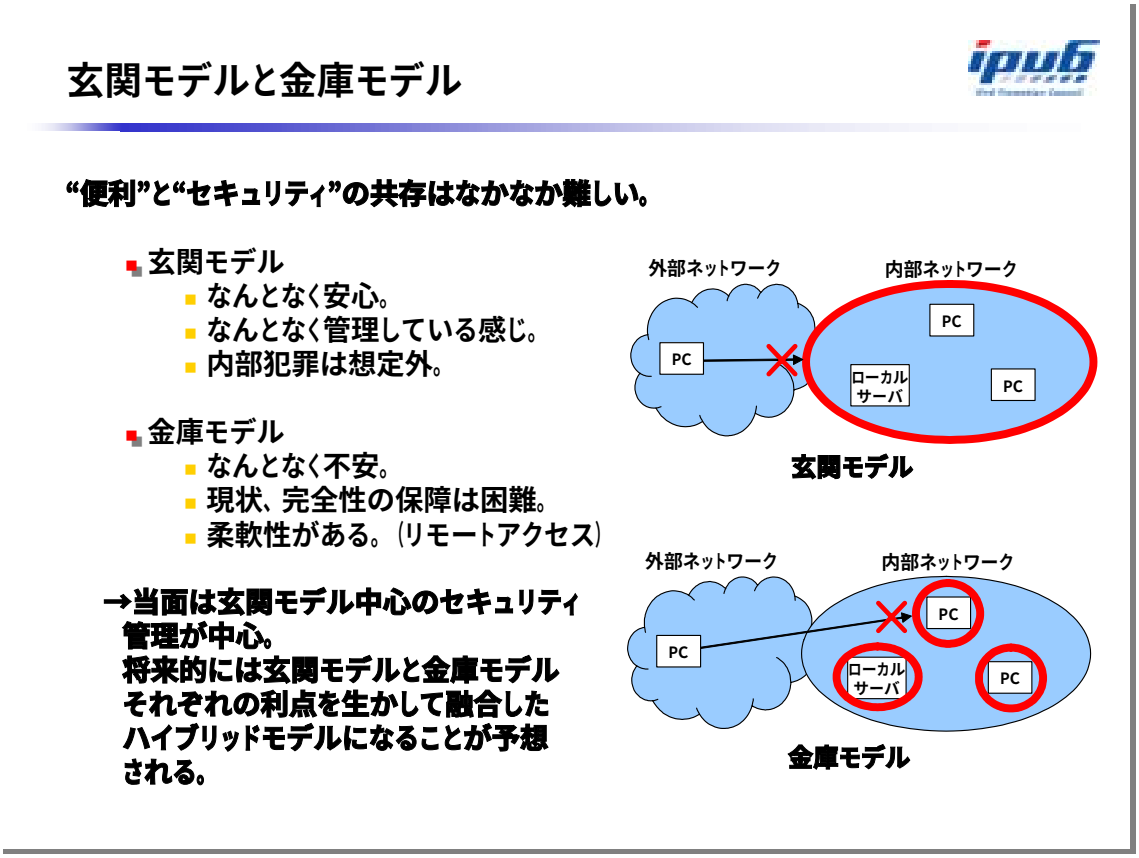
IPv6 では、IPv4 とセキュリティ面でどのような違いがあるでしょうか。IPv6 では IPsec が標準実装されること以外、論理的には IPv4 と同等です。下記のセキュリティ管理項目については、IPv4/IPv6 に関係なく対策の実施が不可欠です。

・不正アクセス防止（ファイアウォール、IDS などの適用）
・情報漏えいの防止（暗号化やパスワードの設定管理(人的管理含む)、など）
・ウィルス対策（アンチウィルスアプリケーションなどの適用）

ただし、IPv4 から IPv6 への移行に伴う、利用するアプリケーションの基本コンセプト（P2P 通信、リアルタイム化、広帯域化など）の変化に対応して、新しいセキュリティポリシーを導入する必要性が大きくなります。

IPv6 におけるセキュリティモデル、およびそれに対応した製品・ソリューションは、まだ完全には確立していません。暫定的なセキュリティポリシーを前提としながら、徐々に実用化していく必要があります。

■玄関モデルと金庫モデル



そもそも、“便利”と“セキュリティ”の共存はなかなか難しい点があります。

プライベートネットワークをパブリックネットワークとの境界で守る「玄関モデル」は、現在のネットワークセキュリティ対策における主流です。なんとなく安心で、なんとなく管理している感じがあります。しかし、ブロードバンド化が進んだ場合にはボトルネックが発生する懸念があります。また、内部犯罪は想定外です。

一方、ネットワークに接続される個々の端末・機器でセキュリティを確保する「金庫モデル」においては、なんとなく不安で、現状、組織としてのネットワーク管理として完全性の保障は困難ですが、リモートアクセスをはじめ、様々な点で柔軟性があります。

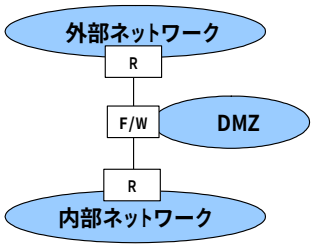
当面は玄関モデル中心のセキュリティ管理が中心となりますが、将来的には玄関モデルと金庫モデル、それぞれの利点を生かして融合したハイブリッドモデルになることが予想されます。

■将来の F/W 構成

将来のF/W構成

＜従来のF/W構成＞

- F/Wが外部と内部を跨るアクセスを集中管理。
- 通過するパケットは、F/Wが全数確認。
- 公開サーバなどは、DMZに配置。



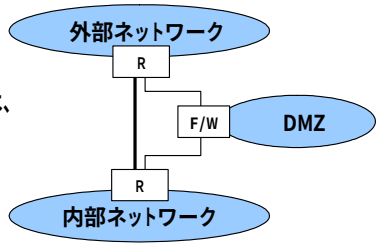
従来のF/W構成

＜問題点＞

- IPv6化と共に多種多様なアプリケーションが導入されることにより、ブロードバンド化が加速し、帯域的にF/Wがボトルネックになる。

＜将来のF/W構成＞

- フィルタリング処理の段階分け。
  - 明らかに通過、もしくは明らかに廃棄のパケットは、ルータで処理。
  - 必要な時だけ、F/Wで詳細チェック。
- 玄関モデルから金庫モデルへ。
  （ボトルネックの解消。）



将来のF/W構成

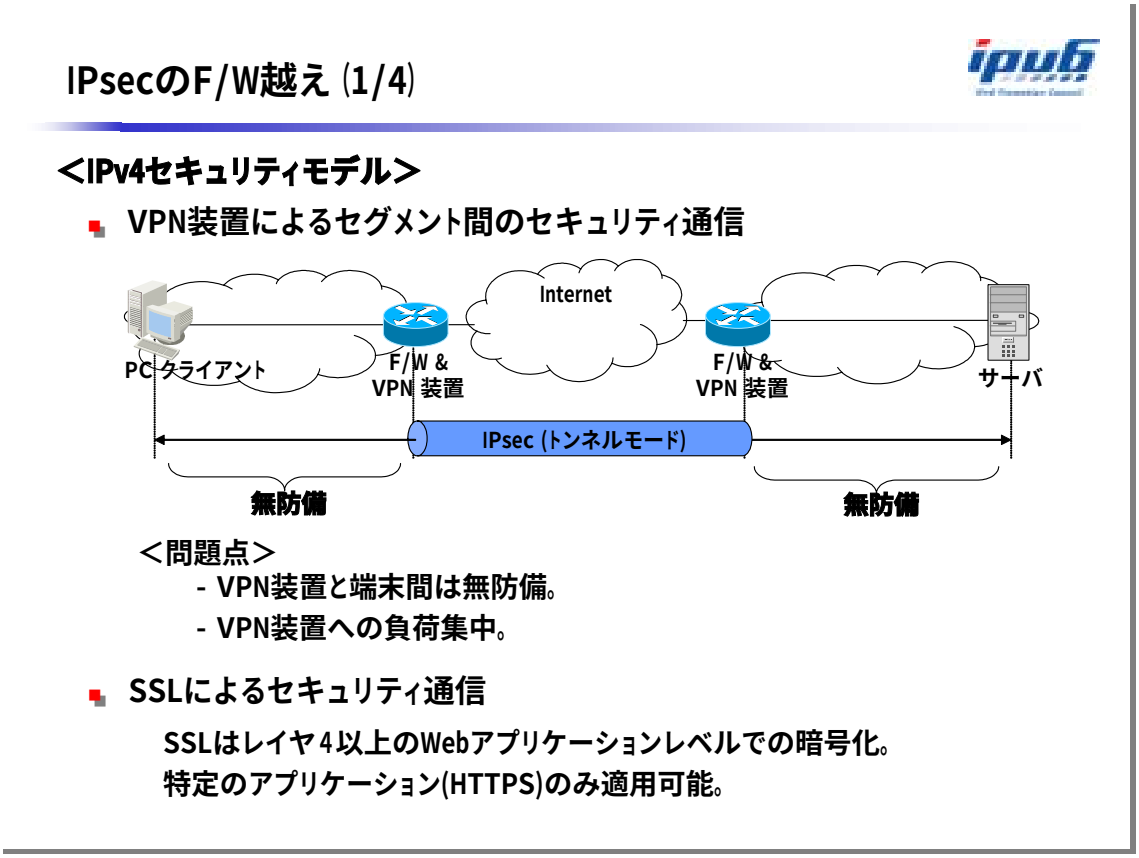
従来は、ファイアウォールが外部と内部をまたがるアクセスを集中管理していました。通過するパケットは、ファイアウォールが全数確認します。そして公開サーバなどは、内部ネットワークとは別セグメントの DMZ に配置しています。

この方法における問題点としては、IPv6 化と共に多種多様なアプリケーションが導入されることにより、ブロードバンド化が加速し、帯域的に F/W がボトルネックになり、これまでのファイアウォール構成では保護しにくい場面が増えてくることが挙げられます。

そこで、将来のファイアウォール構成としては、フィルタリング処理の段階分けを行うことが考えられます。明らかに通過、もしくは明らかに廃棄のパケットは、ルータで処理し、必要な時だけファイアウォールで詳細をチェックするということです。さらに、玄関モデルから金庫モデルへ移行することにより、ボトルネックを解消することができます。

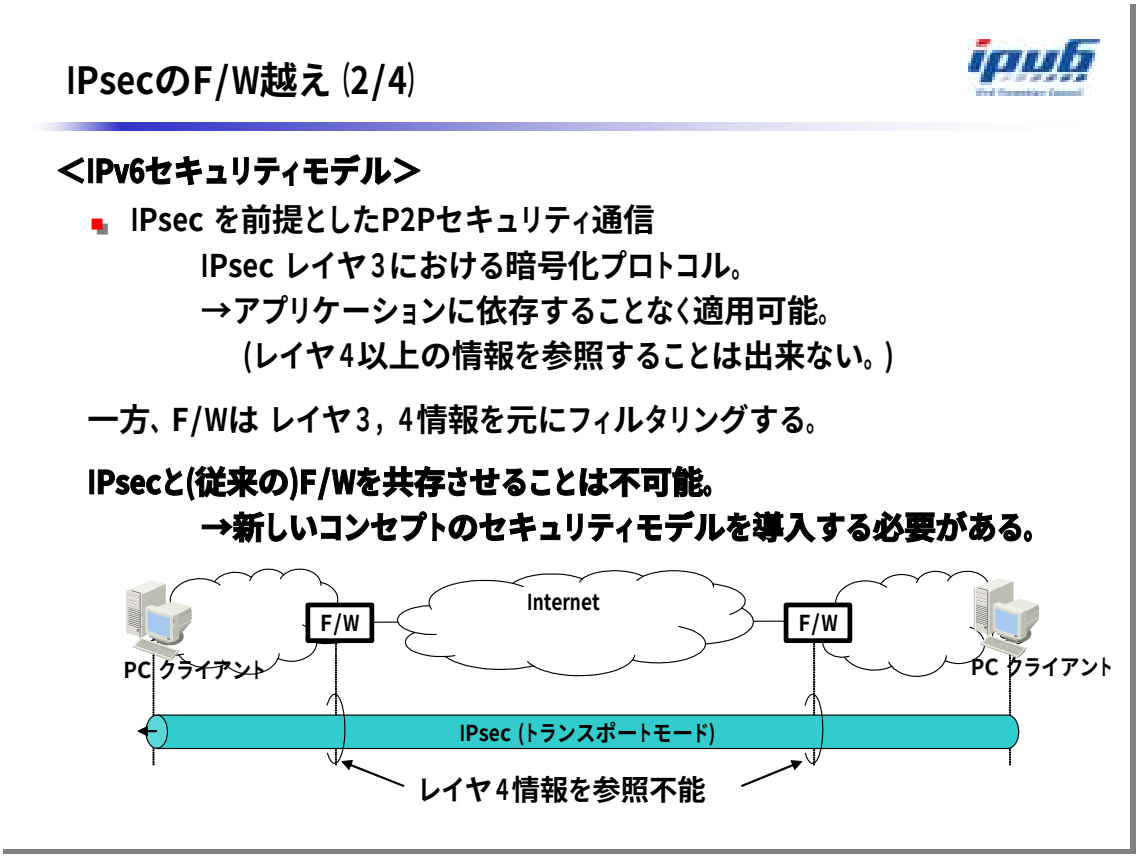
■IPsec の F/W 越え

(1) IPv4 セキュリティモデル



現状では、VPN 装置によるセグメント間のセキュリティ通信が中心です。この方式の問題点としては、VPN 装置と端末間は無防備であり、さらに VPN 装置に処理負荷が集中することが挙げられます。また、現在は SSL によるセキュリティ通信も広く使われていますが、SSL はレイヤ 4 以上の Web アプリケーションレベルでの暗号化であり、特定のアプリケーション（HTTPS）にしか適用できないという制限があります。

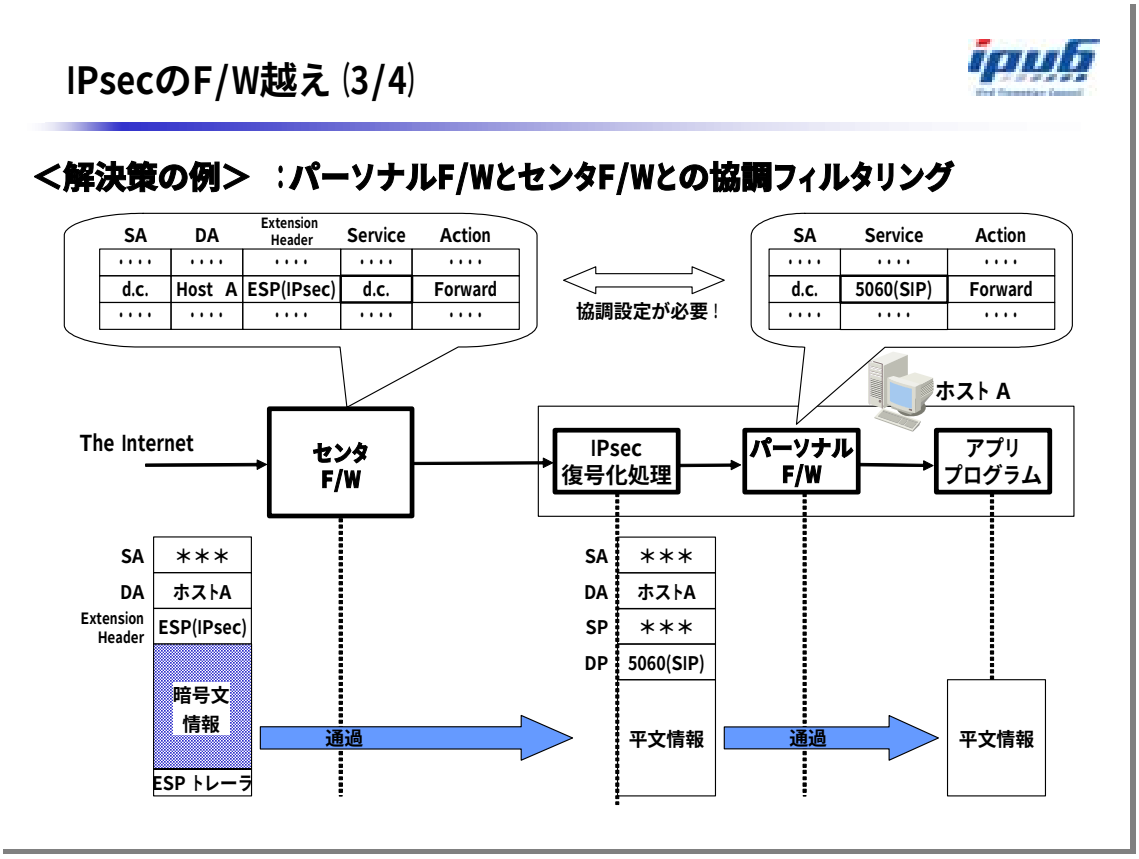
(2) IPv6 セキュリティモデル



IPv6 のセキュリティモデルでは、端末レベルで IPsec がより頻繁に利用されます。IPsec はレイヤ 3 における暗号化プロトコルとして、アプリケーションに依存することなく適用可能です（レイヤ 4 以上の情報を参照することはできません）。

一方、ファイアウォールはレイヤ 3、4 の情報を元にフィルタリングします。したがって、このままでは IPsec と（従来の）ファイアウォールを共存させることは不可能です。このため、新しいコンセプトのセキュリティモデルを導入する必要があります。

(3) パーソナル F/W とセンタ F/W との協調フィルタリング



解決策の一例としては、図に示したように、端末のパーソナルファイアウォールと組織のファイアウォール間での協調処理を行うことが考えられます。つまり、たとえば組織のファイアウォールは特定の端末間の IPsec 通信を通過させるものの、この通信については端末のパーソナルファイアウォールにおいて復号化処理の後確実にフィルタリング処理を行うといった相互連携を実現するのです。

(4) 課題

IPsecのF/W越え (4/4)

＜課題＞

- **F/W 設定**

  個々のF/Wの設定を手動設定することは現実的に不可能。

  ↓

  一定のセキュリティポリシに基づき、ネットワーク全体の整合がとれたF/W設定を自動構築する“F/W マネージャ” 相当機能の導入が必要。

- **ダミーIPsecパケットによるDoS攻撃**

  本来の通信とは関係無い無意味なデータの大量送付により、各端末はIPsecの復号化処理で飽和する恐れがある。

  ↓

  (a) SPI (Security Pointer Index)を確認して動的にセンタF/Wのポリシを変更し、適正な IPsec パケットのみが通過できるようにする。

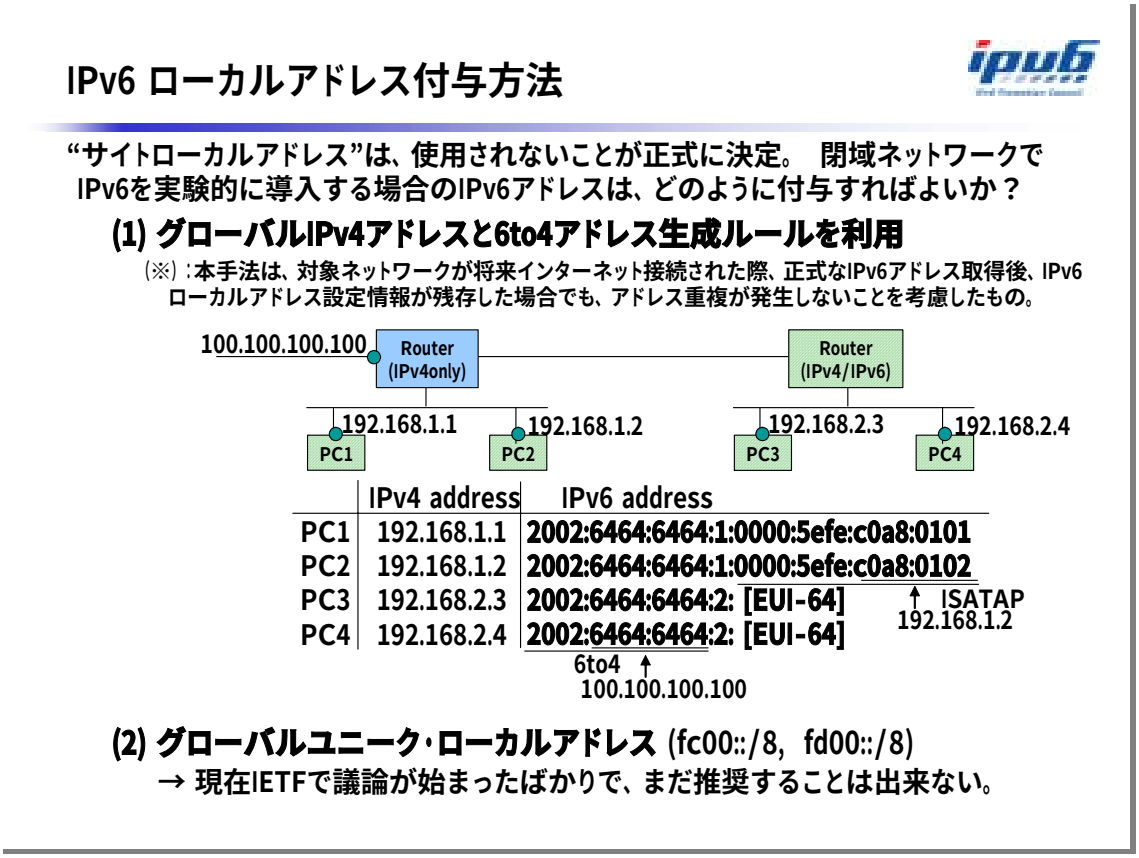
  (b) 各端末にIDS機能を導入し、疑わしいパケットを検知した場合には、動的にセンタF/Wのポリシーを変更する。

この時、組織のファイアウォールにおける IPsec 用の穴あけは、IPsec 通信の必要性に応じてきめ細かく行わなければなりません。しかし、個々のファイアウォールの設定を手動設定することは現実的に不可能です。したがって、一定のセキュリティポリシーに基づき、ネットワーク全体の整合がとれたファイアウォール設定を自動構築する“ ファイアウォールマネージャ ” 相当機能の導入が必要になるでしょう。

また、こうした新しい利用形態の下では、ダミーIPsec パケットによる DoS 攻撃に対する備えも重要になります。つまり、本来の通信とは関係のない無意味なデータの大量送付により、各端末が IPsec の復号化処理で飽和する恐れがあります。 その対策としては、(a) SPI (Security Pointer Index)を確認して動的にセンタ・ファイアウォールのポリシーを変更し、適正な IPsec パケットのみが通過できるようにする。 (b) 各端末に IDS 機能を導入し、疑わしいパケットを検知した場合には、動的にセンタ F/W のポリシーを変更するといった対策が求められます。

6. Tips & Tricks

■IPv6 ローカルアドレス付与方法



IPv6 において、プライベートネットワークにおける利用を想定したアドレスとして考えられていた“サイトローカルアドレス”は、使用されないことが正式に決定しました。それでは、閉域ネットワークで IPv6 を実験的に導入する場合の IPv6 アドレスは、どのように付与すればよいでしょうか。ここでは以下の 2 つの方法を紹介します。

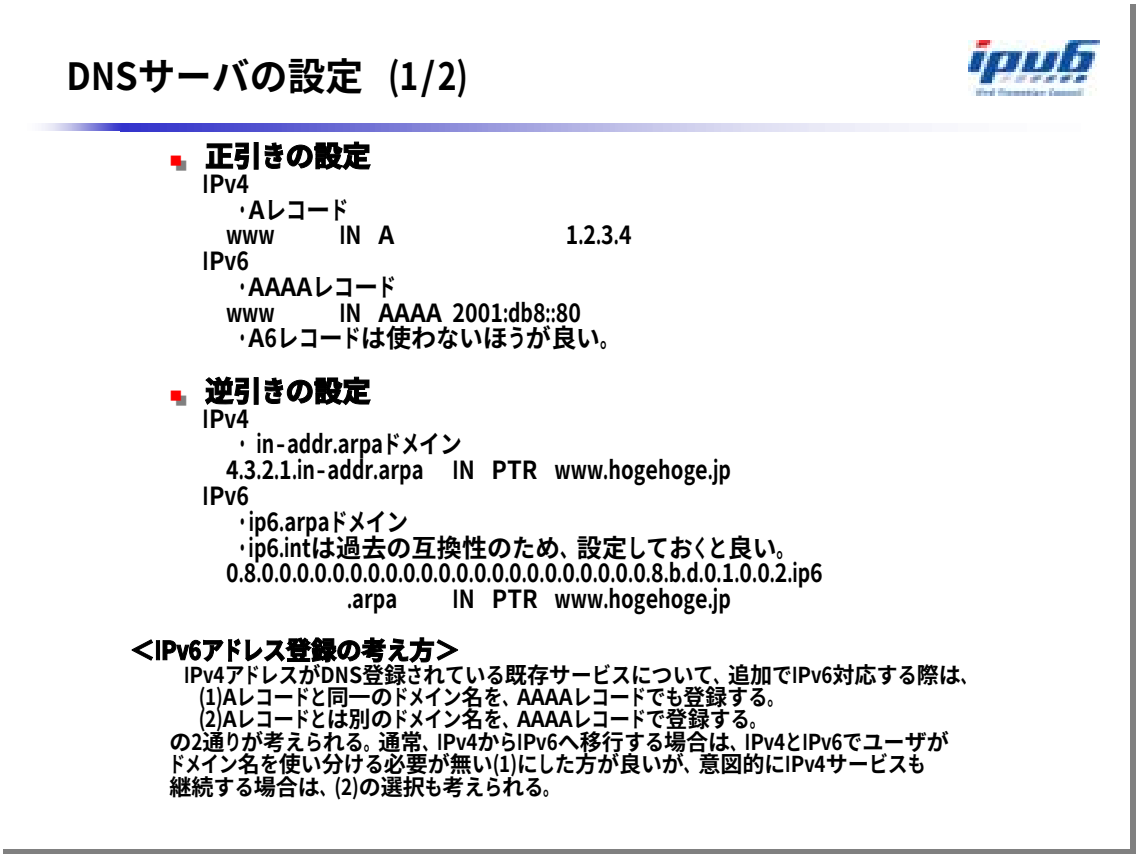
グローバル IPv4 アドレスと 6to4 アドレス生成ルールを利用

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

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

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

■DNS サーバの設定

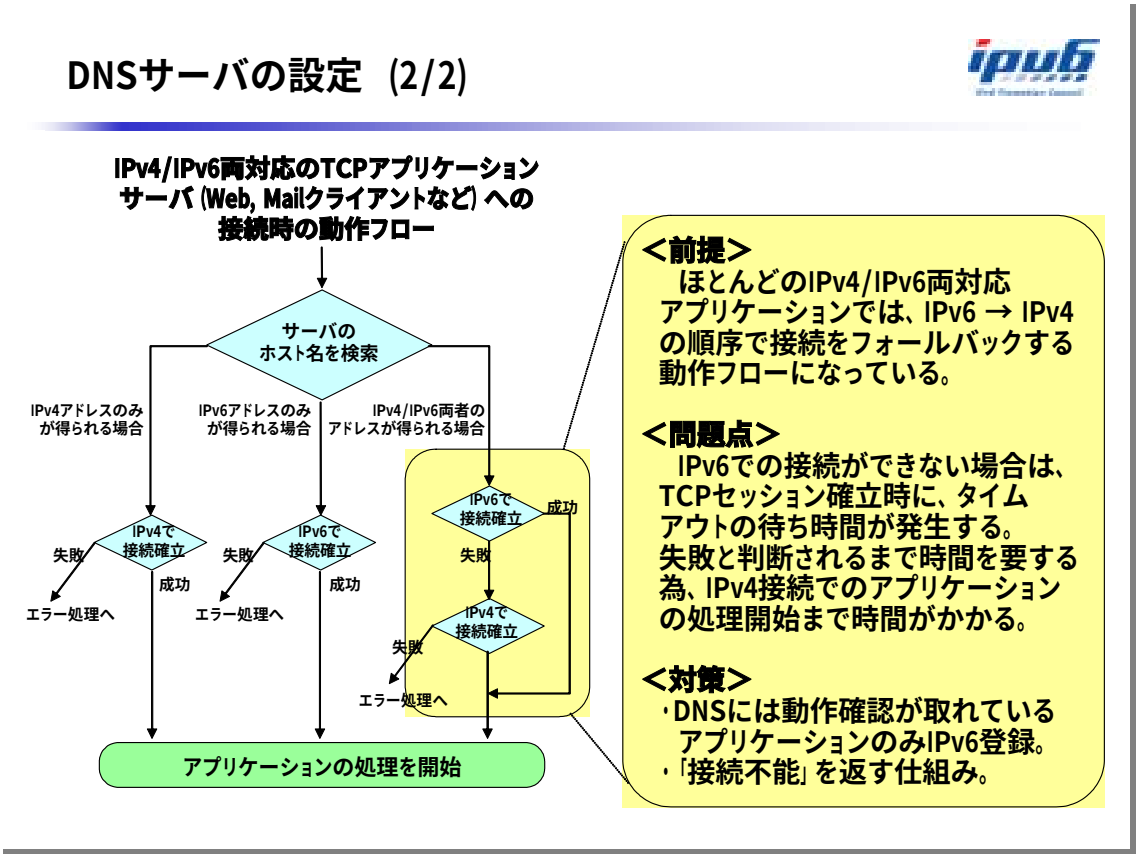


DNS レコードの設定は、上のように行うことを推奨します。

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

1. A レコードと同一のドメイン名を、AAAA レコードでも登録する。
2. A レコードとは別のドメイン名を、AAAA レコードで登録する。

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



IPv6 導入時の DNS 設定にあたって注意すべき点を一つ説明します。

IPv4/IPv6 両対応の TCP アプリケーションサーバ（Web, Mail クライアントなど）への接続時の動作フローは図のようになります。ほとんどの IPv4/IPv6 両対応アプリケーションでは、IPv6 → IPv4 の順序で接続をフォールバックする動作フローになっています。

このフローの問題点は、IPv6 での接続ができない場合は、TCP セッション確立時に、タイムアウトの待ち時間が発生することです。失敗と判断されるまでに時間を要するため、IPv4 接続でのアプリケーションの処理開始まで時間がかかってしまいます。

この問題への対策としては、DNS には動作確認が取れているアプリケーションのみ IPv6 登録をし、「接続不能」を返す仕組みを取り入れることが考えられます。

■MTU ディスカバリについて

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

一方、IPv6 ではパケット配送における経路途中では Fragment が実施されません。経路途中のあるルータでパケットサイズが Too Big となった場合、そのルータが ICMPv6 の Type2「Packet Too Big Message」を送信元に返します。送信元はそのメッセージを受け取り再度適切なサイズにパケットを収めて送信します。したがって、IPv6 インターネット上では ICMPv6 メッセージ（少なくとも Type2）がエンドノードまで配送されないと、通信性がそこなわれる場合があるので注意が必要です。

ISP を含めて、ICMPv6 Type2 メッセージはフィルタリングしない運用を徹底する必要があります。

IPv6 移行ガイドライン（大企業・自治体セグメント）

平成 16 年 5 月発行

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