2005 年 IPv6 移行ガイドライン

大企業・自治体編

2005 年 3 月

IPv6 普及・高度化推進協議会

移行 WG　大企業・自治体 SWG

本ドキュメントについて

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、方法について記述する。

ここで記載される内容は、考え方の例を示すものであり、唯一の解ではない。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た。

目次

1. セグメントの特徴 4

大企業・自治体ネットワークの特徴 4

大企業・自治体ネットワークの分類要素、IPv6 との関連性 4

2. BCP（今すぐできること） 5

2.1　IPv6 ネットワーク環境の先行導入 8

2.2　新規アプリケーション導入に伴う IPv6 導入 23

3. IPv6 普及期のときの目標とする NW＆システム形態＋アプリケーション 32

4. IPv6 普及期に向かうための課題 38

検討メンバ 41

本ガイドラインの改定について 41

1. セグメントの特徴

大企業・自治体ネットワークの特徴

ここで検討対象とする大企業・自治体ネットワークの特徴は以下の通りです。

- 全体ネットワークは特定の専任部門が管理
- ユーザ数が数十人以上の比較的大規模なネットワーク
- 組織内にイントラネットが存在
- 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る
- コスト：費用対効果が特に強く求められる
- セキュリティ：ネットワーク部門が、セキュリティポリシーを厳格に維持管理
- 安定性：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（冗長構成、設備の定期更新）

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・自治体ネットワークの分類要素、IPv6との関連性

(1) インターネットとの接続ポイントの数
- 1箇所
- 複数

→マルチホーム ルーティング

(2) インターネット接続回線の種別
- 専用線
- xDSL, CATV, FTTH

→ISPサービスメニュー

(3) ユーザ数（共有サーバへのアクセス量）
- 100人以下
- 100人以上

→負荷分散装置

(4) 拠点数
- 単一拠点
- 複数拠点

→拠点間接続方法

(5) 拠点間のつなぎ方
- メッシュ型（IP-VPN、広域イーサ）
- スター型（インターネットVPN、専用線）

→拠点間接続方法

(6) サーバアクセス方式
- ASP型
- 1箇所集中型
- 拠点分散型

→ASPサービスメニュー, 負荷分散

(7) 冗長構成（ISP接続回線、基幹装置など）
- 有り
- 無し

→VRRP, OSPF

(8) リモートアクセス
- 有り
- 無し

→リモートアクセスサービス

(9) アドレス運用
- グローバル
- プライベート

→NAT

(10) VoIPの導入
- 有り
- 無し

→SIP, NAT

2. BCP（今すぐできること）

基本方針

基本的考え方

IPv4 と同等の IPv6 ネットワーク環境の確立がターゲットです（当面は IPv4 も従来通り継続して運用)。

ネットワークの使い分けについては､既存アプリは既存 IPv4 ネットワークシステムで継続運用し、新規アプリは新規 IPv6 ネットワークシステムで試行後、実運用します。

導入方法

初めは、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ます。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。

そして、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。当面の暫定的なセキュリティに関する考え方は下記の通りです。

緩和モデル

現状の IPv4 ベースの F/W 設定に、IPv6 対応の設定を同等レベルで追加、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、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

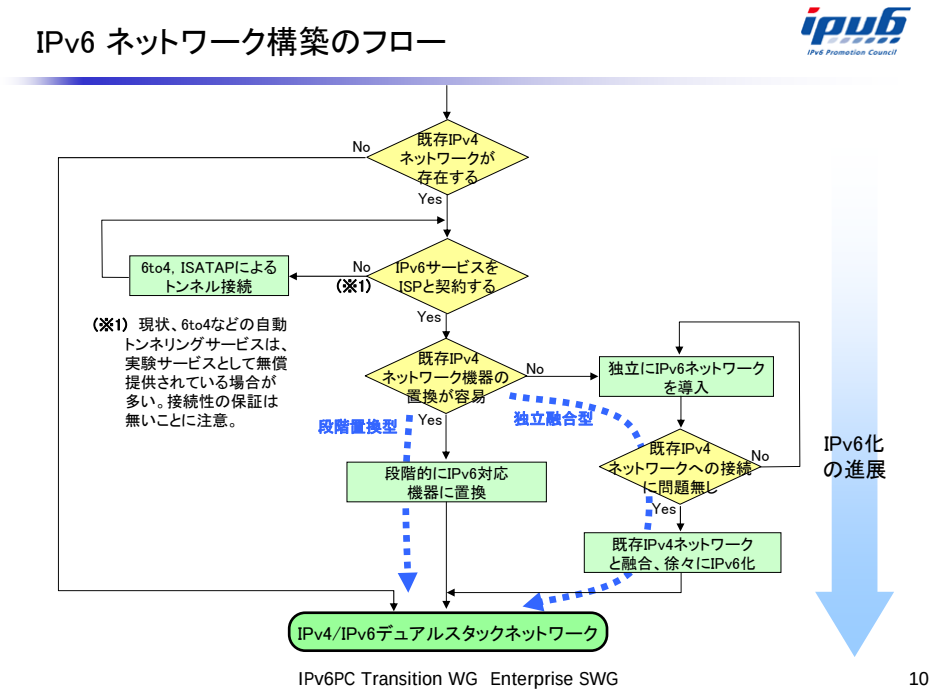
このモデルでは、既存ネットワークと新規 IPv6 ネットワークの接続を認めません。第一段階では、現用ネットワークから独立した IPv6 ネットワークを構築します。

大企業･自治体の IPv6 セキュリティポリシーが、更に実用的なレベルまで確立されるまでは、IPv6 ネットワーク及びこれに接続する端末上で、企業秘密情報、個人情報などを取り扱いません。

“IPv6 セキュリティポリシーの整理は、直近の最重要課題である！”

IPv6 ネットワーク構築のフロー

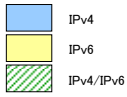
大企業や自治体における IPv6 ネットワークへの移行では、段階置換型と独立融合型の 2 つのパターンが考えられます。

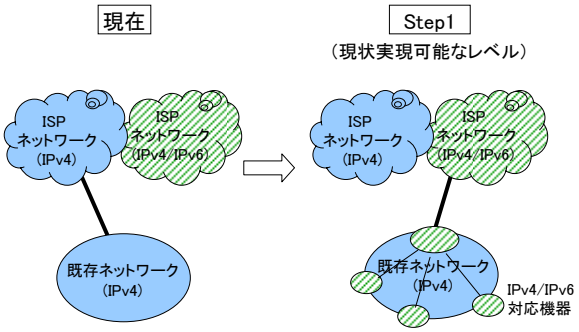


段階置換型の移行パターン

段階置換型の移行パターン

既存ネットワークを段階的にIPv6化し続け、基幹ネットワークは全てIPv4/IPv6デュアルスタック対応にする。



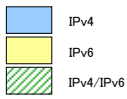


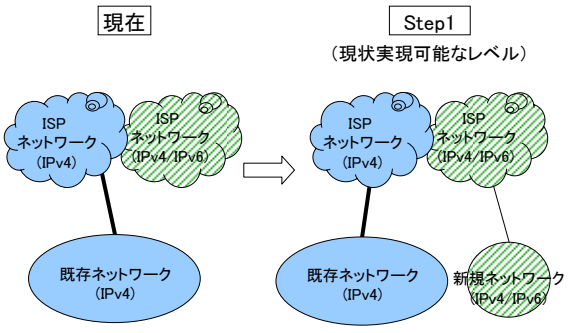
・既存IPv4ネットワークの一部を段階的にIPv6対応機器に置換していく。

独立融合型の移行パターン

独立融合型の移行パターン

独立したIPv4/IPv6デュアルスタックネットワークを、既存ネットワークと融合させ、徐々にトラフィックを移行させていく。





・既存IPv4ネットワークとは独立に、IPv4/IPv6ネットワークを構築。

“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としては、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。

2.1　IPv6 ネットワーク環境の先行導入

IPv6 対応サービス・機器について

“IPv6 の基本的な環境(要素技術)は既に整っている”

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

主要ファイアウォールでは、基本的なパケットフィルタリング機能が IPv6 対応しました。実用レベルでの付加機能も充実してきています。しかし、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の検討が必要です（→セキュリティガイドラインの I-1～2、J-1～4 参照)。

また、現状では、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ないことにも注意が必要です。

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、クエリパケットの IPv6 化にまでこだわる必要はありません（AAAA レコード対応が重要)。

暫定的には、IPv6 対応の外部 DNS を参照する手もあるかもしれません。

gTLD(Generic Top-Level Domains)、ccTLD(Country code Top-Level Domain）において、ルート DNS サーバが IPv6 対応しています(.jp、.kr など)。

ルータや FW に実装されている DNS については、一部好ましくない動作をするものも存在するため、確認が必要です（→6 章 Tips “DNS サーバの設定" 参照)。

その他サーバ

Web や Mail(※1)などは、主要ソフトウェアにおいて IPv6 対応済みとなっています。

ネットワーク管理サーバは、MIB が IPv6 に対応（SNMP は IPv4 ベース）しています。

PC・PDA

主要な OS は、ほぼ IPv6 対応済です（ただし、機能的な対応レベルは様々)。新規購入、OS 最新化に伴い IPv6 化します。E2E 通信を考慮して、端末レベルでのセキュリティ対策を徹底する必要があります。

（※1）：　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です。

IPv6 グローバルアドレスの取得

IPv6 アドレスの取得方法

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、グローバル・プレフィックスの割当てを受けることが可能です。（※1）

現在有効なアドレスポリシーでは、企業や自治体に割り付けられるアドレス空間は、契約する上流の ISP より割り当てられる、１つもしくは複数の/48 の大きさとなります。

しかし、企業の規模が大きい、またはグループ企業でイントラネットを構成している、などのケースにより、/48 を割り当てたいサイトが 200 以上となる規模のネットワークを構成できる企業ネットワークを管理運用する企業は、アドレスポリシーの初期割り振り基準に見合うので、RIR（地域レジストリ、日本は APNIC の管轄）に対し、/32 の独立アドレス空間を申請することができ、審議によって取得することも可能です。

一方、自治体では、その提供するサービスの公共性や組織の定款からアドレス空間の独立性を維持することも審議では考慮され、200 以上の/48 割り当てが可能な規模に至っていなくても/32 空間のアドレス割り振りがなされる可能性もあります。ただし、APNIC より/32 空間を取得した場合は、ISP と同様に/48 空間の割り当て管理、APNIC への報告業務を負うことになります。

（※1）：　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 アドレス取得に関する詳細情報

JPNIC のサイト：

http://www.nic.ad.jp/ja/translation/ipv6/20040714-01.html

IPv6 普及・高度化推進協議会 リモートコントロールノードアドレス SWG のサイト：

http://www.v6pc.jp/jp/wg/remoteSWG/index.html

IPv6 グローバルアドレスの設計

基本的な考え方

/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(※1)であるが、将来の展開を考慮し、下記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

（※1）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、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。

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 に対応しています。上位機種では、OSPFv3 に対応しているものもあります。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。

大企業・自治体ネットワークにおける IPv6 ルーティングプロトコル

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、OSPFv3 を導入します。

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。

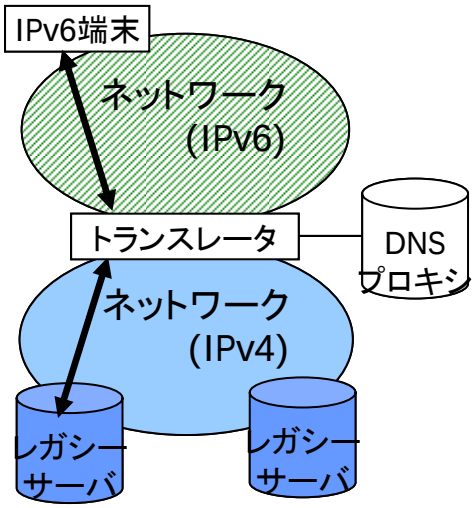
ライブ中継や放送などのサービスでマルチキャストの利用を想定する場合は、PIM-SM などのマルチキャストルーティングプロトコルに対応した機器を選択します。

トランスレータ

特徴

NAT-PT 方式、TRT 方式が商用化されています。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。

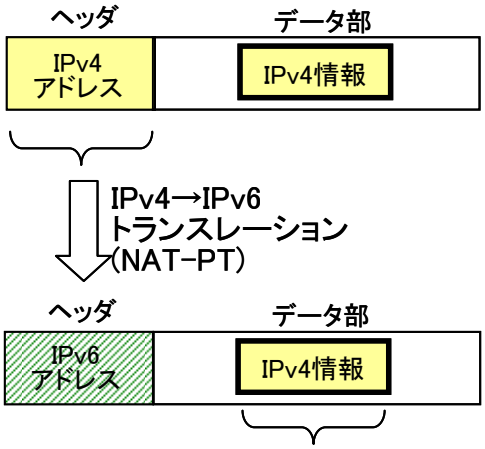
DNS プロキシを利用して、FQDN（Fully Qualified Domain Name）を使って通信相手を指定可能です。レガシーシステムのサーバ設定を変更することなく、IPv6 対応にすることができます（膨大な IPv4 システムの資産をそのまま利用可能）。



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（下図参照）。IPv4→IPv6 パケット変換時は、MTU（Maximum Transmission Unit）の設定にも注意が必要となります。通信相手には FQDN が必要です。

また、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。



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 IPv6overIPv4 トンネルを生成します。

自動トンネリング

DTCP（Dynamic Tunnel Configuration Protocol）

この方式では、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　フリービットの 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(※1)、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生成します。往路と復路の経路が同一になる保証がありません。

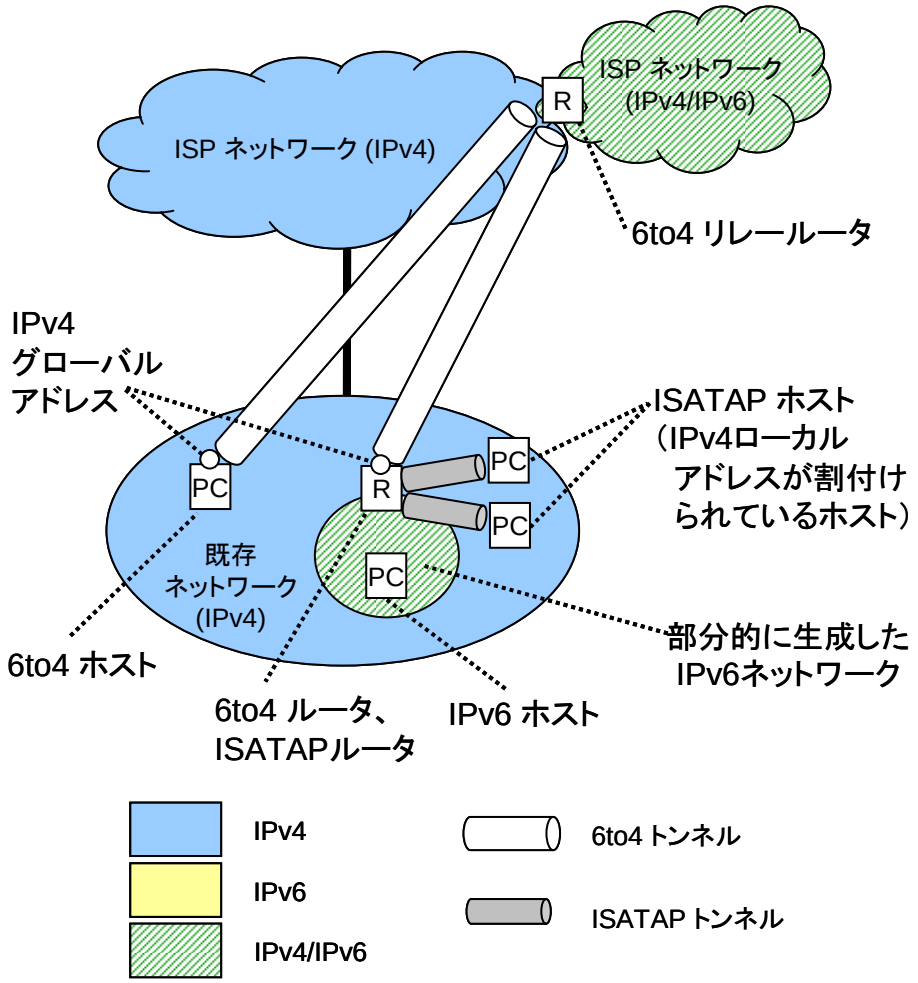
ISATAP

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（6to4、ISATAP など）を利用した IPv6 導入イメージ



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 トンネルを生成します。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 トンネルを生成します。

トンネル生成区間に F/W 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です。

比較的容易に IPv6 導入可能だが、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。ただし、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。

（※1）WinXP では、ホストにグローバル IPv4 アドレスが付与される場合、自動的に 6to4 トンネルが生成される。

境界部分の IPv6 化

既存ネットワークにおける境界部分に求められる機能は、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 です。

IPv4 では、ファイアウォールや NAT が上記機能を実現しています（アドレス変換機能以外は、IPv6 でも必要です)。

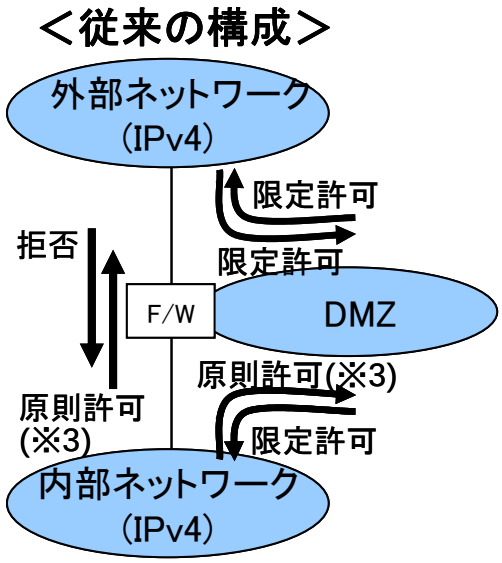
IPv6 導入にあたっては、既存 IPv4 部分は変更せず、IPv4/IPv6 対応ルータ(可能であればファイアウォール)を追加導入するのが理想的です。新規 IPv4/IPv6 対応ルータでは、IPv6 トラフィックのみを処理することとし、原則として IPv4 と同等(※1)のフィルタリング設定をします。

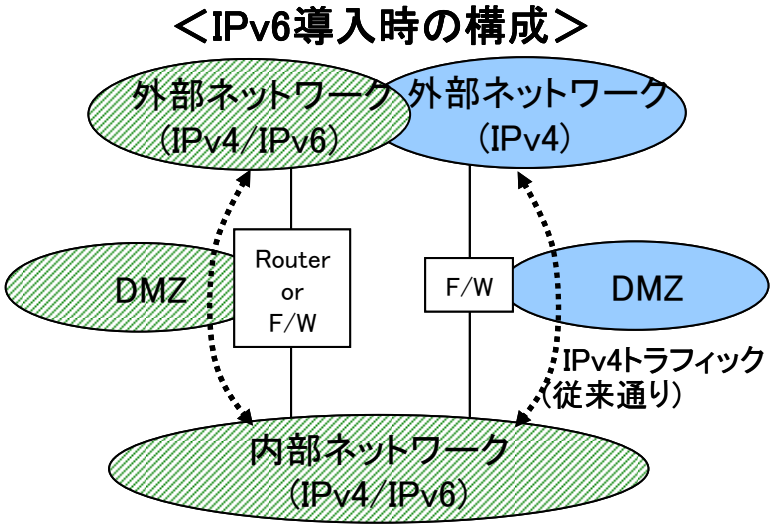
IPv4 トラフィックは、既存 IPv4 部分で処理(※2)します。

(※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。尚、ICMP に関するフィルタリング設定については、 「6 章　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デグレを防ぐこと、および、万一 IPv6 側に障害が発生しても既存サービスを継続することが目的です。ロギング、ウィルスチェック、IDS 機能においても、同様の考え方をします。

(※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見られます。

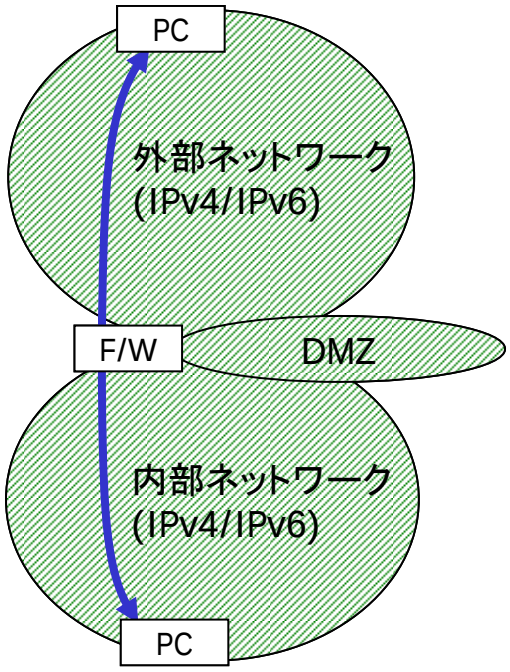




フィルタリング

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）のが基本です。



・E2E 通信について

ファイアウォールを経由する 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です (→セキュリティガイドライン：A-1～3 参照)。

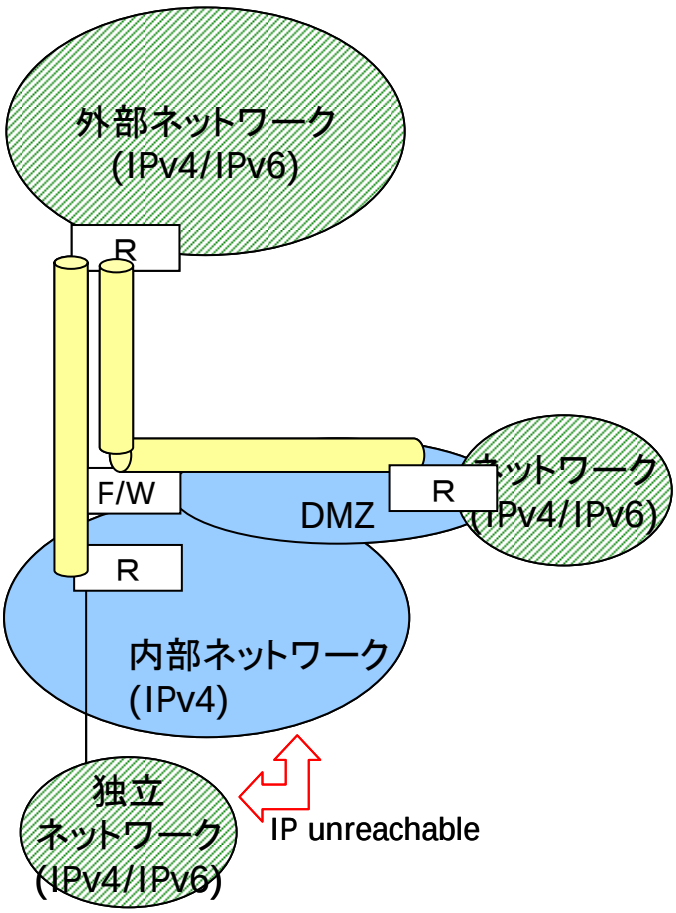
ファイアウォールを経由する IPsec ベースの E2E 通信については、今後の課題です。試験的に許容する場合は、限定した端末において特定のアクセス(IP アドレスでフィルタリング)のみを通過させるべきです。その際、終端装置には、パーソナル F/W などのセキュリティ対策を導入すべきです（→セキュリティガイドライン：A-4 参照)。

IPv6 未対応 F/W の場合

・IPv6overIPv4 トンネルについて

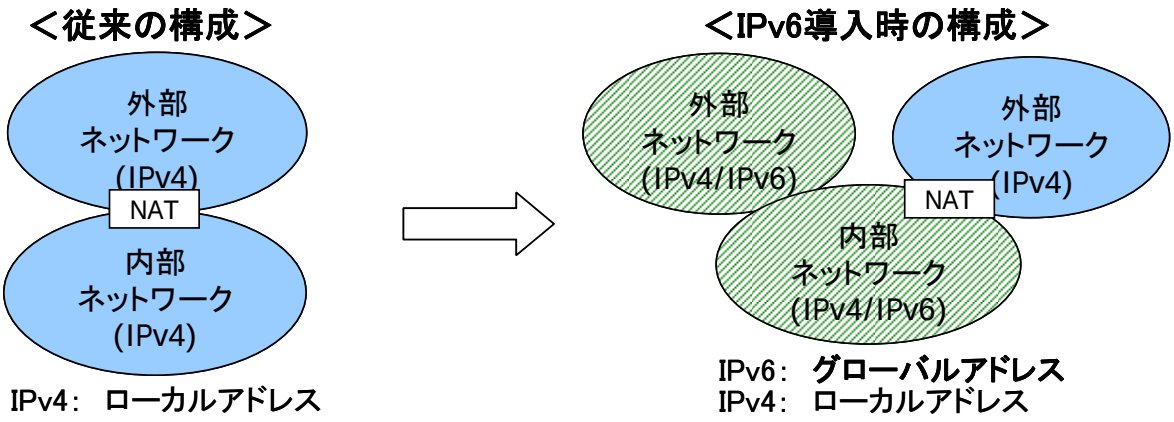
基本は、IPv6overIPv4 トンネリングアクセスを DMZ 向けに対して許可（IP プロトコル番号 41 の通過を許可）し、DMZ における部分的な IPv6 対応セグメントを生成します。この IPv6 対応セグメントでは接続ホストを限定し、特別なセキュリティ管理を実施すべきです。

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）で試行すべきです。



NAT

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



・アドレス情報の秘匿について

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、今後の課題です。

(※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においてその利用方法については検討が必要です（→セキュリティガイドライン：D-1 参照)。

リモートアクセス

現状のリモートアクセス方式として、次が挙げられます。

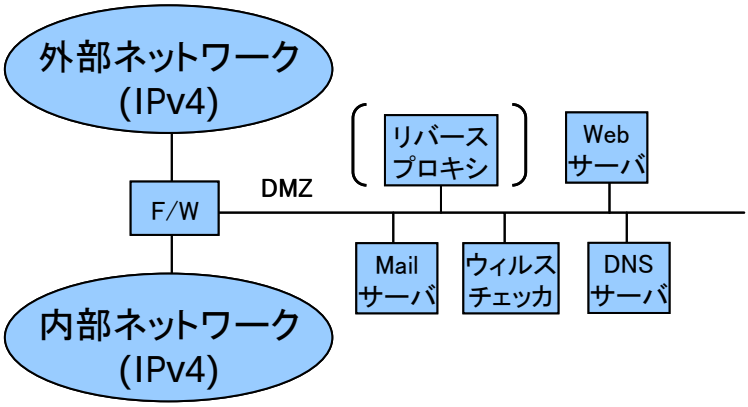
(a) (企業が持つ)NAS に電話をかける
(b) (プロバイダが持つ)NAS に電話をかけて、そこから一括で L2TP によるアクセス
(c) インターネット VPN(トンネルモード)
(d) SSL-VPN

現状、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。

DMZ の IPv6 化

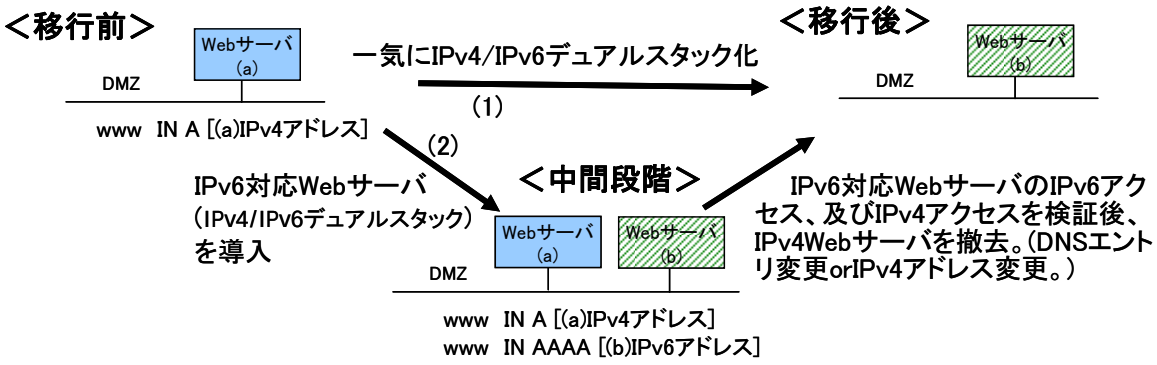
Web サーバ

ファイアウォール（F/W)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(代わりにリバースプロキシ)、Mail 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。



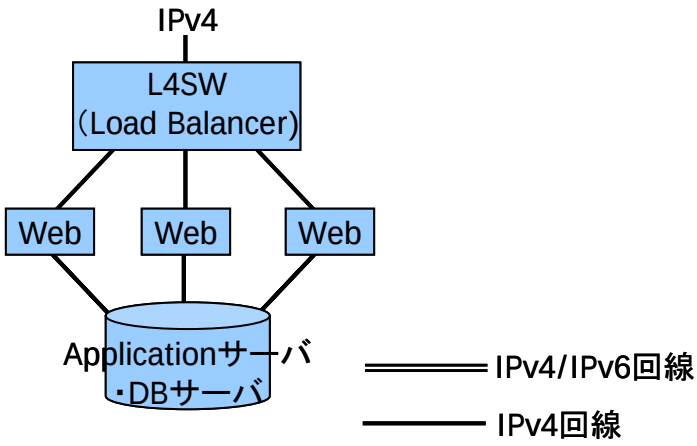
・Web サーバの IPv6 化

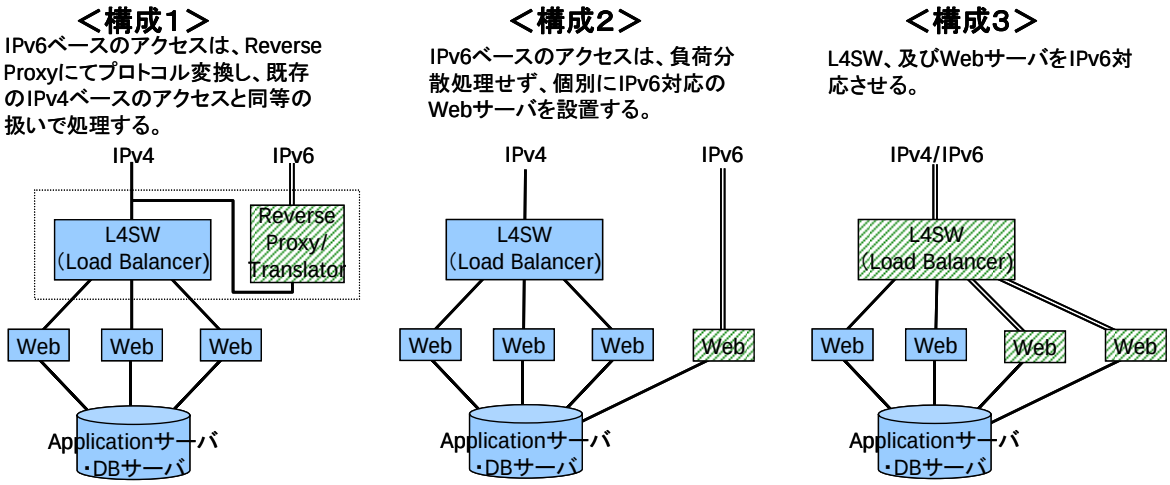
Web サーバの IPv6 化は、Apache2.0 をはじめとして、バージョンアップにより比較的容易に実現可能です。実運用の Web サーバに対して、(1)一気に IPv4/IPv6 デュアルスタック化する場合と、(2)一定期間、IPv4Web サーバと、IPv6 対応 Web サーバ(IPv4/IPv6 デュアルスタック)とを併用する場合との、2 通りの IPv6 移行パターンが考えられます。



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、下記＜構成 1＞～＜構成 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。





拠点間接続方式

拠点間の接続方式とデュアル、トンネルの利用可能性の関係は、下表の通りです。

	デュアル（IPv6/IPv4）	トンネル（IPv6 over IPv4）
フレームリレー	○（※1）	○
専用線	○（※1）	○
IP-VPN	－（※2）	○
広域イーサネット	○（※1）	○

※1　終端装置の IPv6 化で対応可能（IP 非依存のはず。ただし、サービス提供者へ確認要）
※2　現状 IPv6 対応しているサービスなし

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ることができます。

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です。

端末管理

端末アドレス情報・DNS 情報の管理について

IPv4 と IPv6 それぞれにおける、端末へのアドレス設定や DNS アドレスの通知の方法は、以下の通りです。

	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ある場合は、インタフェース識別子を EUI-64 で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。ただし、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です。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となります（4 章 IPv6 普及期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)。

※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）

2.2　新規アプリケーション導入に伴う IPv6 導入

アプリケーションの IPv6 対応の進め方

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します。

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 化します(※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 化します。

> ※1　ただし現時点では、たとえば 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れます。

IPv6 らしいアプリケーションとは

IPv6 らしいアプリケーションとしては、各種の P2P アプリケーションがまず考えられます。

P2P アプリケーションの種類	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ー）	○	○	○
グループウェア	○	○	－
サーバレス　ファイル共有	○	○	－
メンテナンス／モニタリング	○	○	－
マルチキャストストリーミング	○	－	－
固定アドレス（Mobile IP）	○	○	－
テレビ会議	○	○	－

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す。IPv6 契約をして必要なトラフィックのため、ファイアウォールに穴を開けるのみです。IPv6 電話の外部接続により、これから広まると考えられる IPv4 電話の外部接続と比較してコストを削減できます。

効果として、外線 GW（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）が考えられます。

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により、セキュリティを確保します。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。

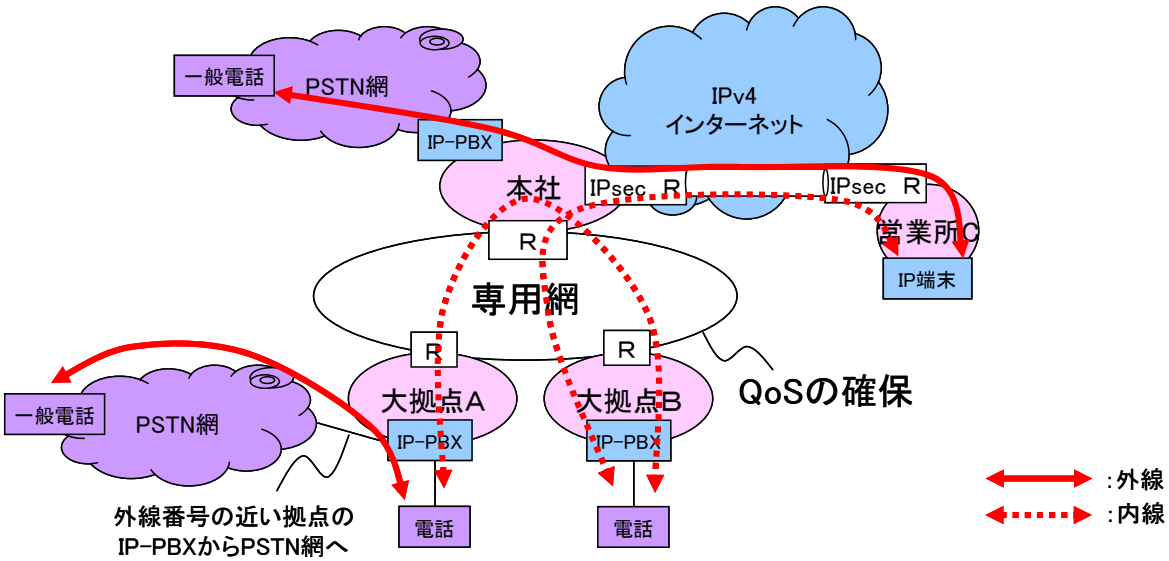
IP 電話に限らず、何かの APL について、その GW の負荷がネックなる場合、○○ソリューションとして、同じ論理で構築が可能です。

2004 年 6 月、VoIPv6 のサービスを約 300 拠点，約 2 万台の端末に対して適用する事例が報告されました。

現状の IP 電話導入パターン

現状では、IP 電話は主に内線電話に利用されています。外線の IP 電話接続はこれからと言えます。大規模拠点は、QoS 確保のため専用線相当の接続を行います。営業所・支店は、インターネット VPN で接続します。

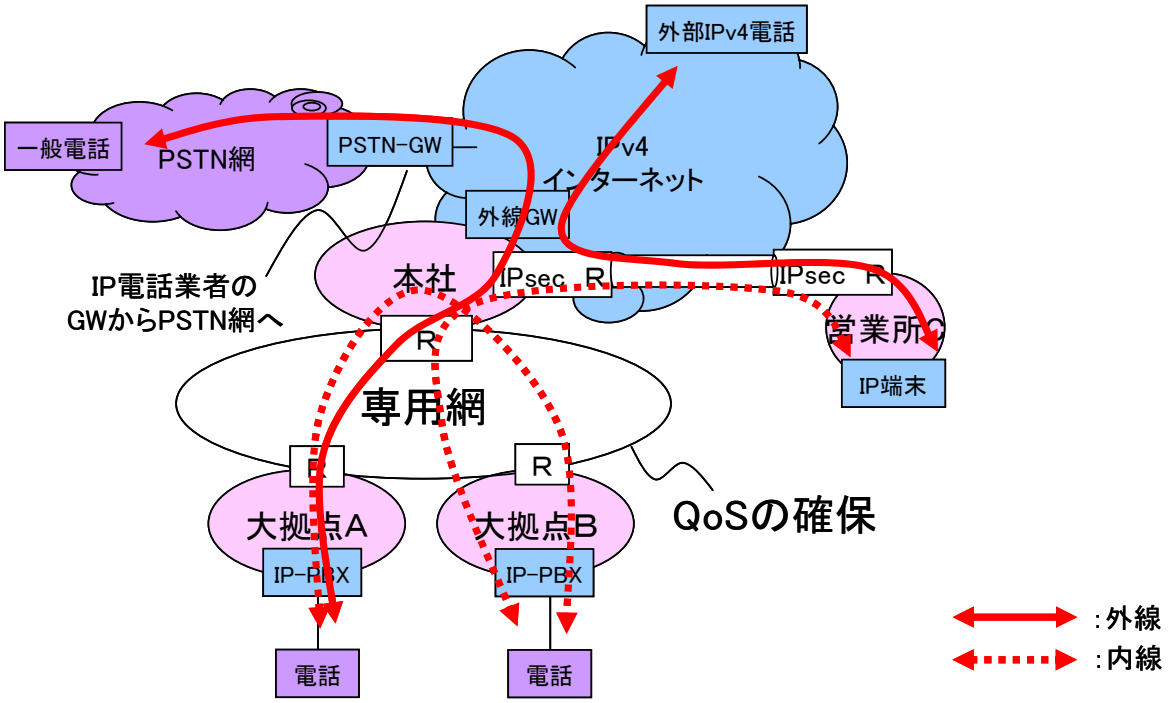
問題点は営業所・支店向けの通信トラフィックの複雑化にあります。



IPv4 による IP 電話の拡張（外線接続）

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、外線ゲートウェイを経由します（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必須です。通話品質確保のためには、コスト増になります。



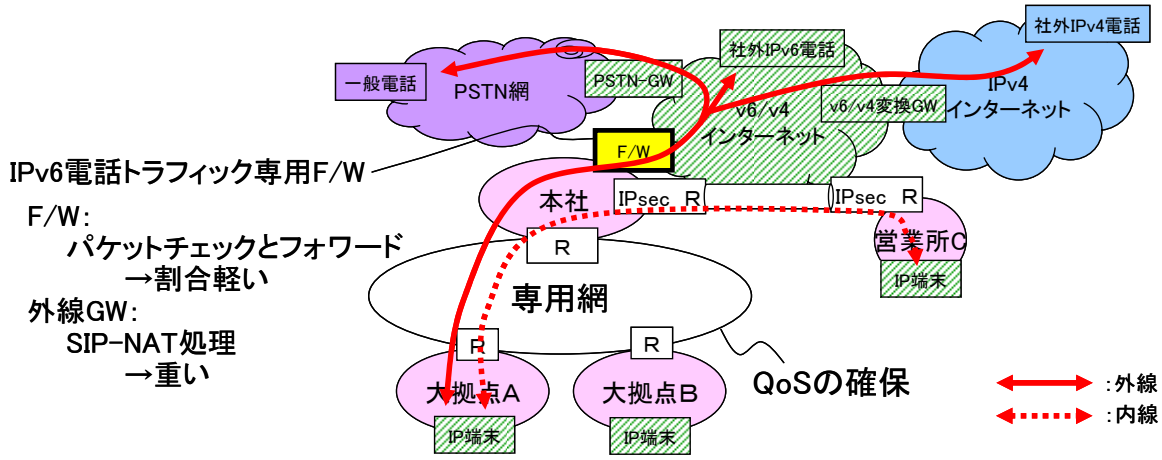
VoIPv6 ソリューション　～大規模拠点向け～

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します。

IPv6 外線は、外線ゲートウェイを通らない　→ファイアウォールを通る

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ちます。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。

メリットは、本社・外線ゲートウェイの負荷軽減と、それによるコスト削減です。

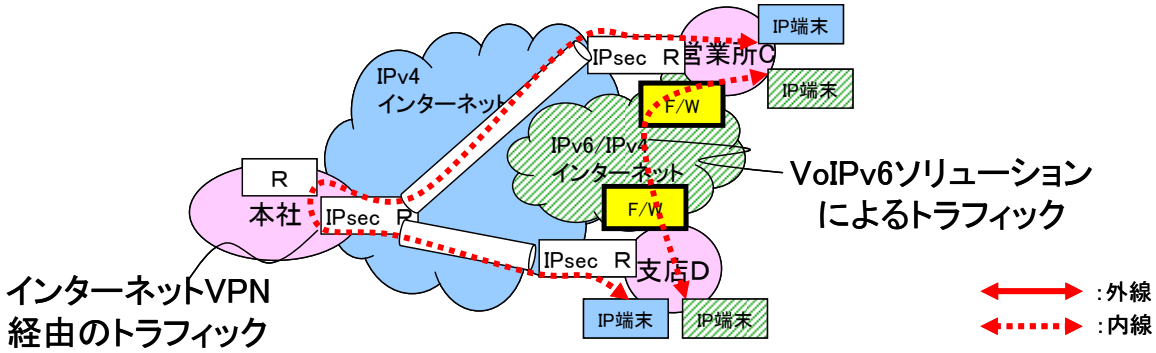


VoIPv6 ソリューション　～営業所・支店向け～

営業所・支店への、インターネット VPN 経由のトラフィックを単純化します。

拠点ファイアウォールは、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ちます。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。

メリットは、新たな IPv4 アドレスが不要でコストが削減できることです（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)。インターネット VPN 経由の通話トラフィックが単純化される利点もあります。



VoIPv6 ソリューション　～もう１つのメリット～

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。

例：100 人の職場の場合

サーバ／ルータ／プリンタ／無線 AP 用（固定割り当て）：50 個

PC 用(DHCP 割り当て)：150 個　（合計 200 個＝/24 で運用可能）

IP 内線電話機を 120 台追加→合計 320 個のアドレスが必要(/24 ではオーバフロー)

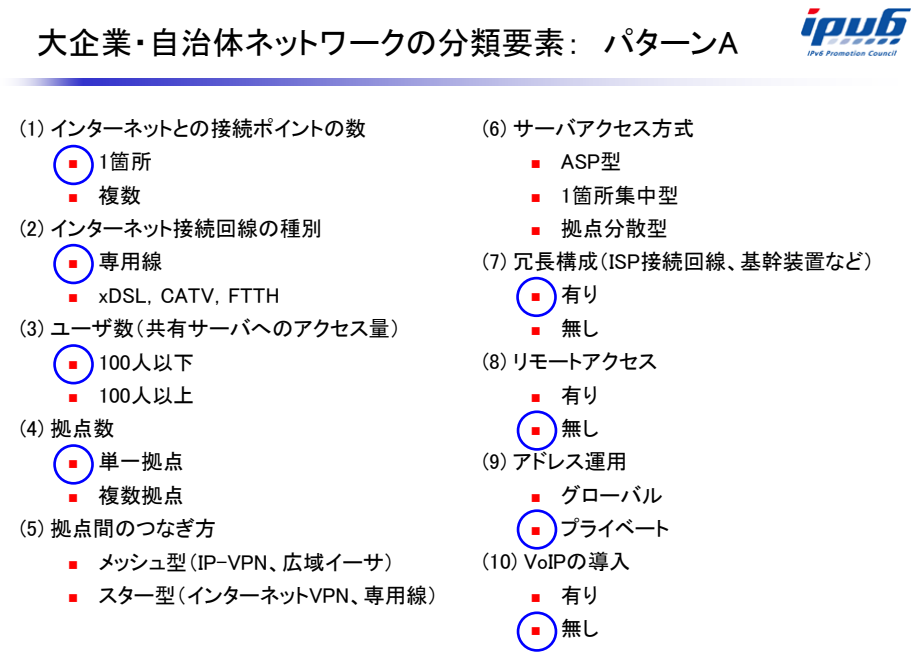
IPv4 の場合は、サブネットの再設計が必要となるため、サブネットマスクを変更します。あるいは別セグメントを追加します（＝IP 電話機を別セグメントとして定義)。

いずれの場合も再設計のコストは大です。

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)は不要となります。

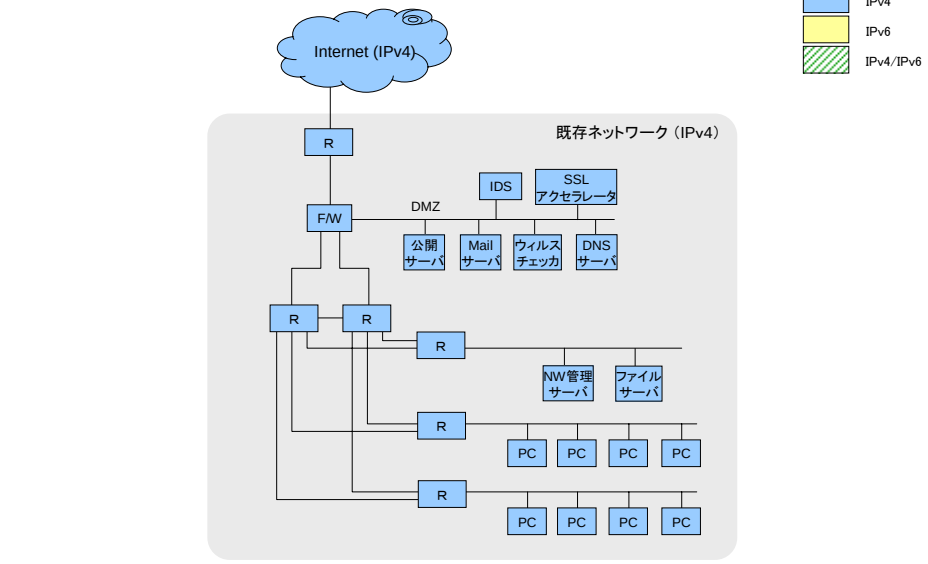
2.3　具体的な IPv6 導入イメージ

大企業・自治体ネットワークの分類要素：パターン A



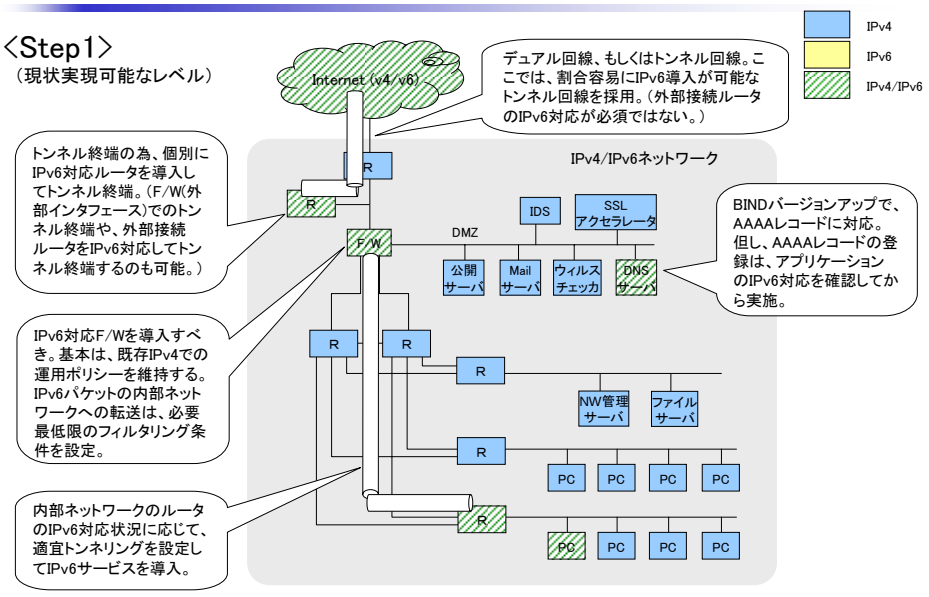
大企業・自治体ネットワークの例：パターンＡ

大企業・自治体ネットワークの例： パターンA



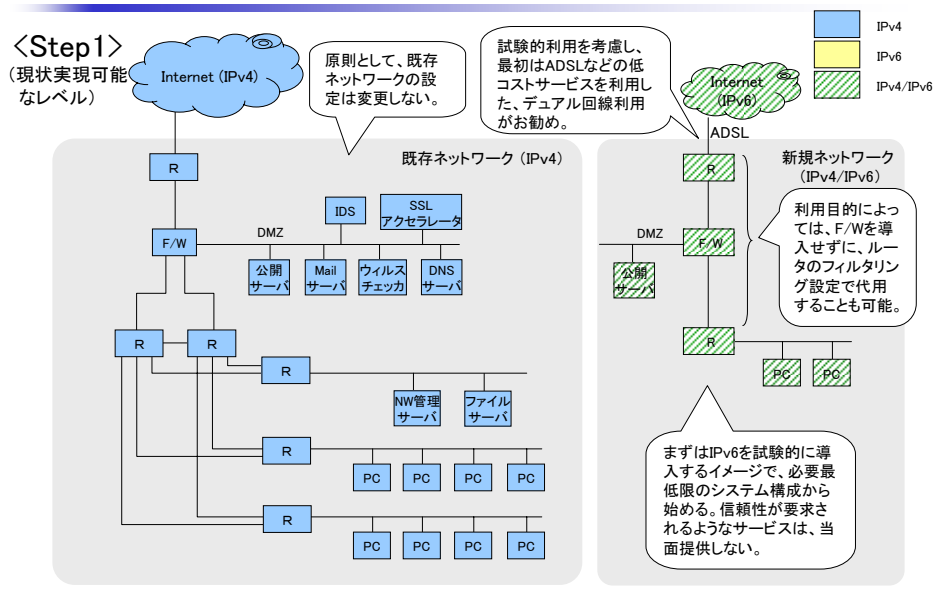
段階置換型： パターンＡ

段階置換型： パターンA



独立融合型： パターンＡ

独立融合型: パターンA



大企業・自治体ネットワークの分類要素：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

(1) インターネットとの接続ポイントの数
- 1箇所
- ○ 複数

(2) インターネット接続回線の種別
- ○ 専用線
- xDSL, CATV, FTTH

(3) ユーザ数（共有サーバへのアクセス量）
- 100人以下
- ○ 100人以上

(4) 拠点数
- 単一拠点
- ○ 複数拠点

(5) 拠点間のつなぎ方
- ○ メッシュ型（IP-VPN、広域イーサ）
- スター型（インターネットVPN、専用線）

(6) サーバアクセス方式
- ASP型
- ○ 1箇所集中型
- ○ 拠点分散型

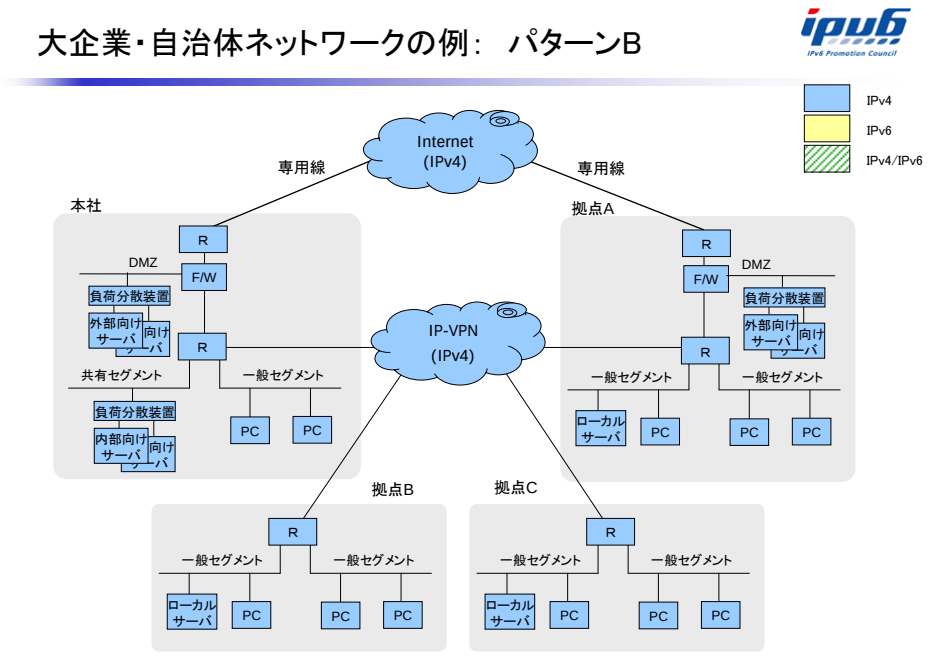
(7) 冗長構成（ISP接続回線、基幹装置など）
- 有り
- ○ 無し

(8) リモートアクセス
- 有り
- ○ 無し

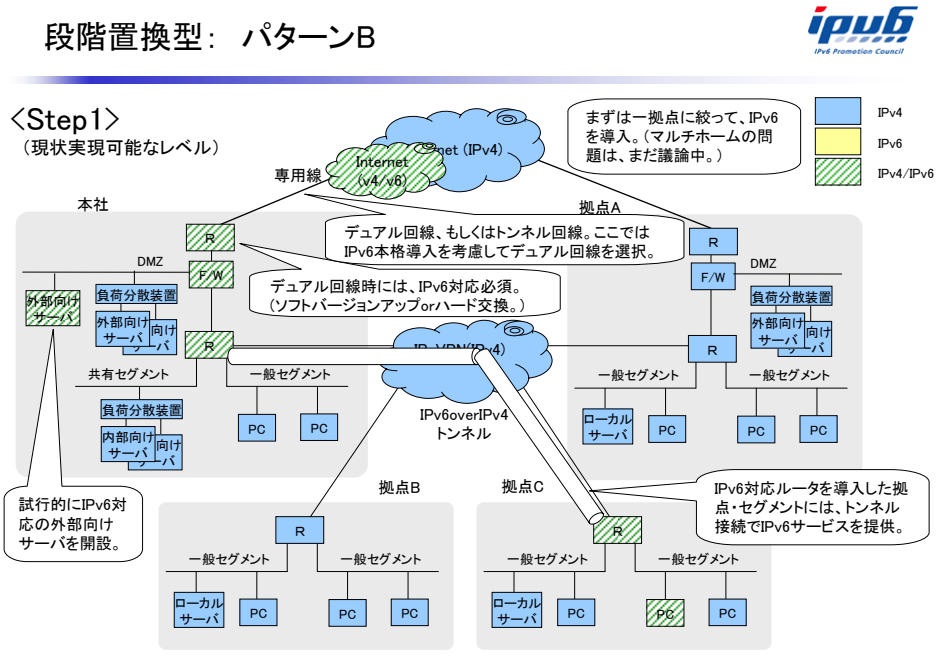
(9) アドレス運用
- グローバル
- ○ プライベート

(10) VoIPの導入
- 有り
- ○ 無し

大企業・自治体ネットワークの例：パターンＢ

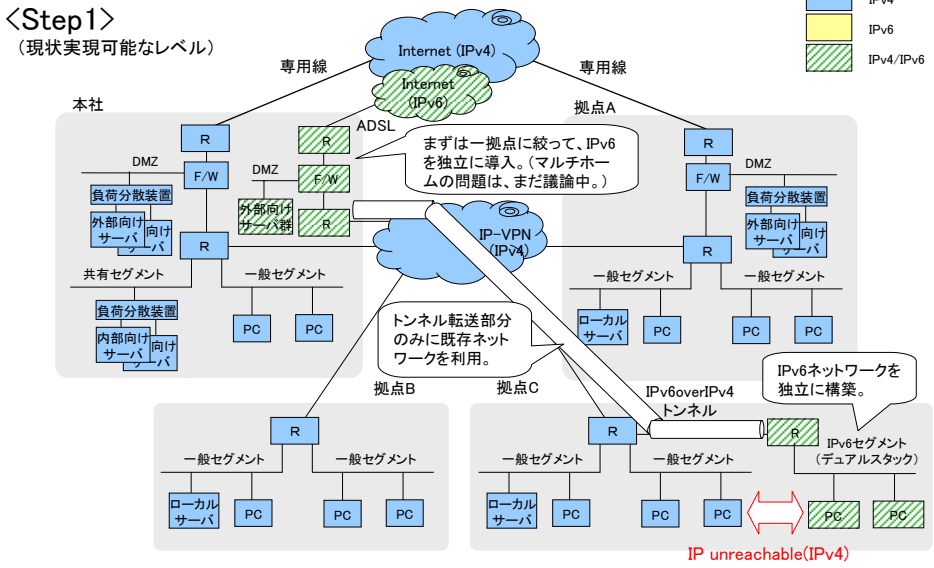


段階置換型： パターンＢ



独立融合型： パターンＢ

独立融合型: パターンB



3. IPv6 普及期のときの目標とする NW＆システム形態＋アプリケーション

IPv6 普及期において想定される IPv6 利用環境と基本方針

予想される IPv6 利用環境

IPv6 普及期に予想される利用環境としては、次の点が挙げられます。

IPv6 ネットワーク環境の充実
・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）
・大型～小型ルータの製品バリエーション充実。
・基本 OS の IPv6 機能本格対応（モバイル、IPsec、）
・各種 IPv6 対応アプリケーションソフトが普及
・ファイアウォール、IDS などのセキュリティ対策製品の充実

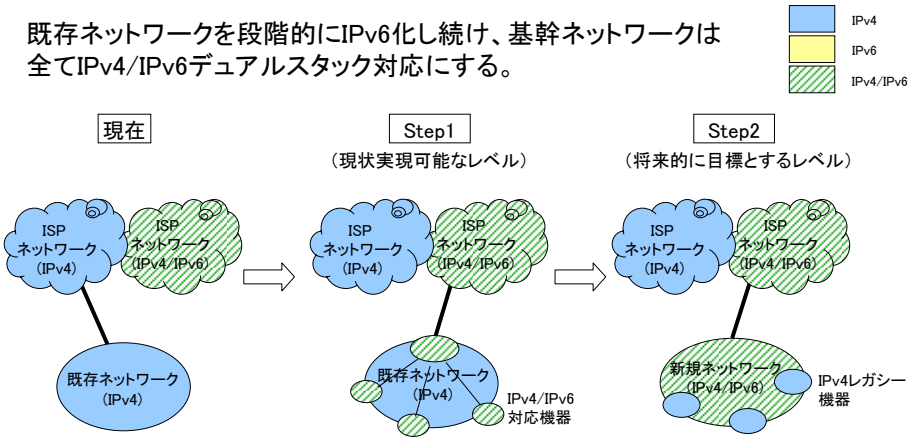
新しいネットワークの枠組みの普及
・non-PC のネットワーク接続。（ユビキタス化の進展）
・組織単位のセキュリティ管理から個人単位のセキュリティ管理へ

IPv4/IPv6 デュアル環境でのセキュリティポリシーが確立
・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
・IPv6 ベースの不正行為が本格化?

段階置換型の移行パターン

段階置換型の移行パターン

既存ネットワークを段階的にIPv6化し続け、基幹ネットワークは全てIPv4/IPv6デュアルスタック対応にする。

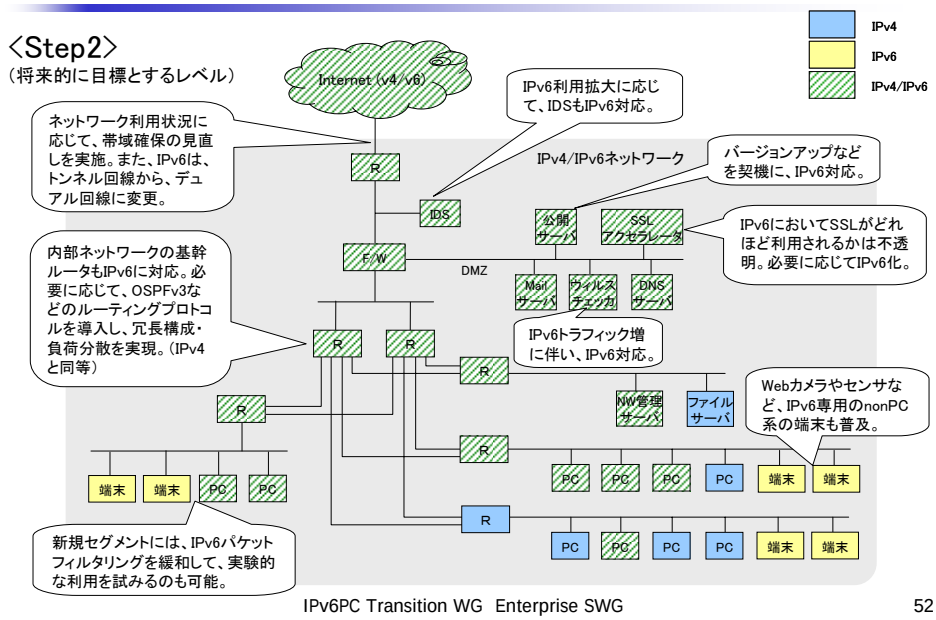


・既存IPv4ネットワークの一部を段階的にIPv6対応機器に置換していく。

・IPv4からIPv6へ移行の進展。
・IPv4レガシー設備が残存。

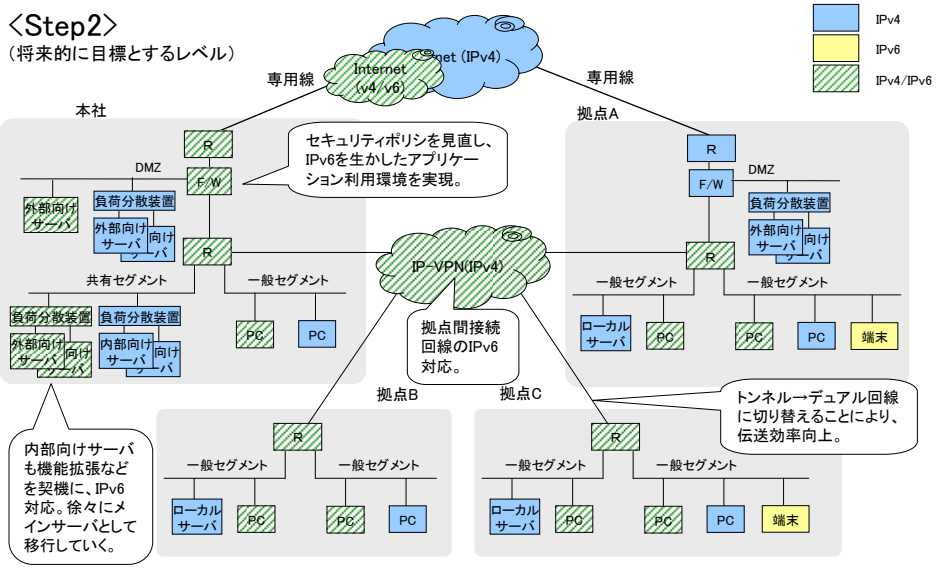
段階置換型： パターンＡ

段階置換型： パターンA



段階置換型： パターンＢ

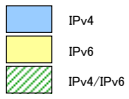
段階置換型: パターンB

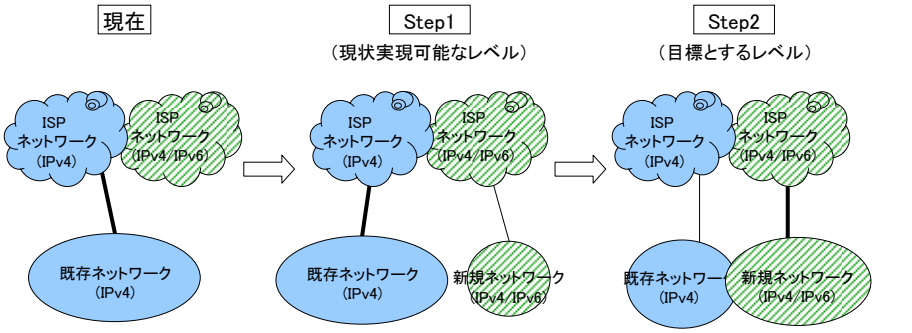


独立融合型の移行パターン

独立融合型の移行パターン

独立したIPv4/IPv6デュアルスタックネットワークを、既存ネットワークと融合させ、徐々にトラフィックを移行させていく。

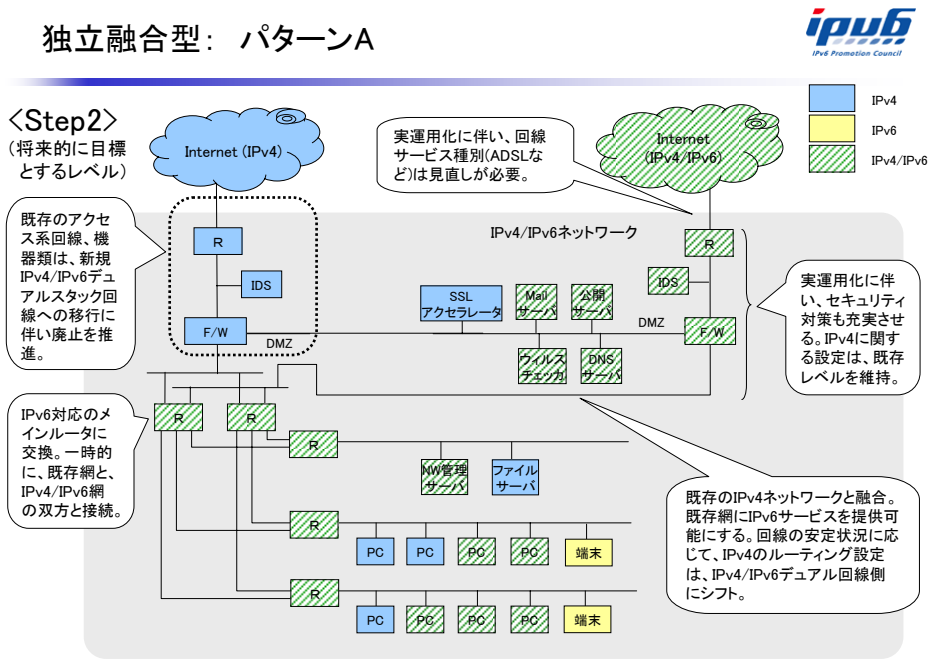




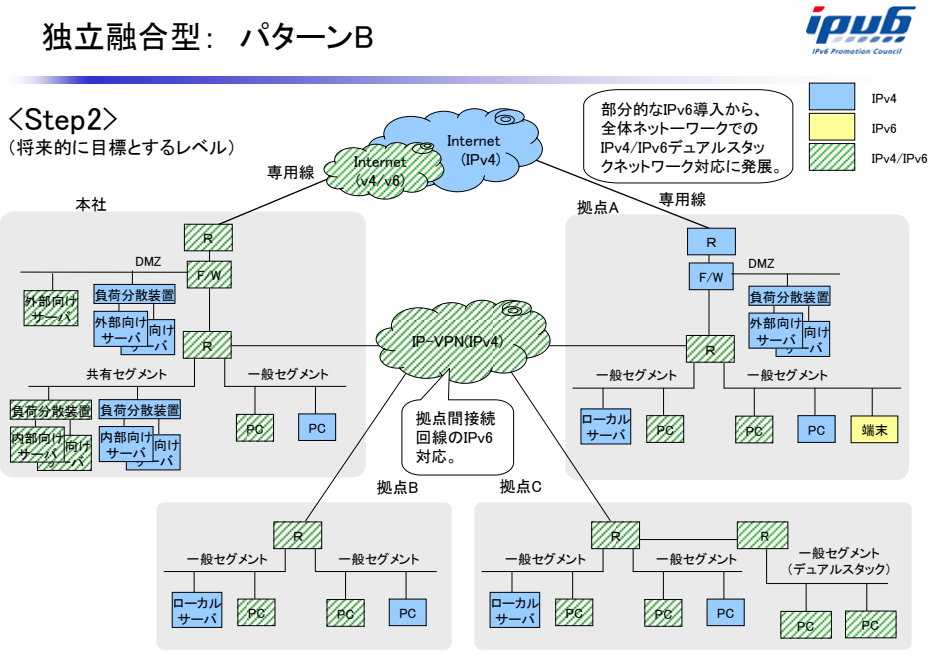
・既存IPv4ネットワークとは独立に、IPv4/IPv6ネットワークを構築。

・既存IPv4ネットワークと新規IPv4/IPv6ネットワークの融合。
・徐々に新規IPv4/IPv6ネットワーク中心へ移行。

独立融合型： パターンＡ



独立融合型： パターンＢ



アプリケーション：IPv6 で実現したいこと

「Plug & Play + Secure + Manageable なネットワーク」

理想の IPv6 環境

・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。
・管理者は、容易に端末の所有者/場所を同定可能。
・管理者は、エンドユーザの設定を一括管理可能。

ネットワーク構成

・ネットワークトポロジーは特に変更無し。
・端末の場所は頻繁に変更可能。

プロトコルスタック

・Dual Stack が基本。
・Pure-IPv6(+ legacy サーバだけ reverse proxy)
  * IPv4+ IPv6 の運用コスト v.s. アプリの IPv6 化
    コストのトレードオフ。
  * IPv6-only 端末もそのうち出てくる。

セキュリティ

・E2E 通信を許可する場合の、端末毎の認証方法やアクセス管理方法。
・外部との間のＥ２Ｅの暗号化に関する、制限方法。
・管理者は組織のセキュリティポリシーに基づき、柔軟な通信制限、チェックを実現したい。

IPv6 らしさの実現に求められる要件

・モビリティの扱い方
・動的な名前登録(Dynamic DNS or SIP)
・MIPv6

E2E 通信（SIP などの利用）

・VoIP(内線,外線)
・テレビ会議
・ファイル共有
・IM

他の端末からのアクセス制御方法

・Personal Firewall
・外部からのアクセス

・社員から外部アクセス（IPsec, F/W）
・機器メンテアクセス（別回線）
・内部アクセスのセキュリティ
・ソーススプーフィング攻撃対策
・端末直収ルータにてフィルタリング
・異常な RA をフィルタリングする Layer 2 switch
・Privacy Extension 対策
　→どこまで何を認めるべき?

4. IPv6 普及期に向かうための課題

マルチホーム

マルチホームのメリット

マルチホームでは、インターネットへの接続に冗長性が確保されます。また、経路最適化や負荷分散が設定可能です。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ました。

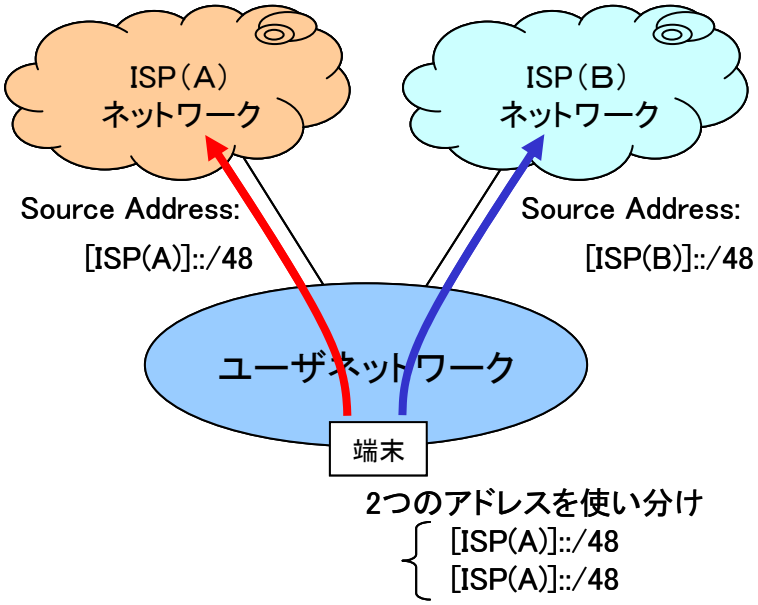
IPv6 のアドレスポリシー

ルーティングの経路集約を重視するため、階層（ツリー）構造のアドレス管理を行います。すべての一般ユーザは、一意の ISP からアドレスを取得します。
→原則として、2 通り以上の経路は発生しません。

問題点

各端末にマルチプレフィクスを割当て、Source Address Selection で対応します。端末に知的なアドレス選択アルゴリズムが必要で、ISP 回線障害時の処理が困難です。

ISP 側にパンチングホールを設定すると、経路情報が増大します。



ネットワークアクセス制御

IPv6 ネットワークでは、多種多様な機器のネットワーク接続が想定されます。

メンバ PC、プリンタ、非メンバ PC/PDA、ホワイトボード、複写機、照明、空調、センサ、監視カメラ、TV…

機器毎に異なるレベルのアクセス制御を設定したい！

すべての機器を同一レベルで管理する必要はない！

というニーズが生まれます。

解決策

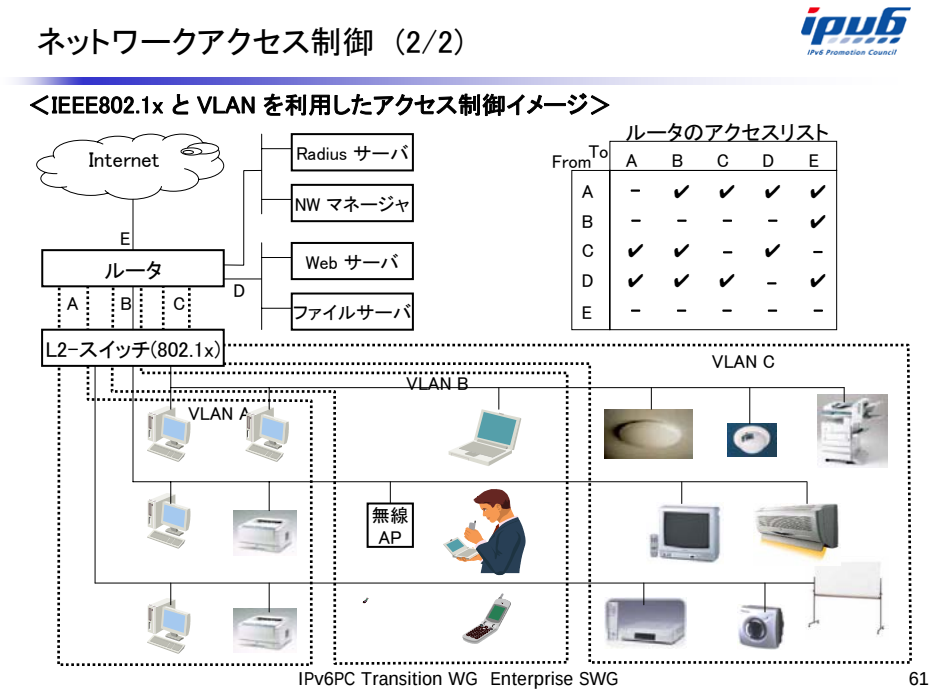
VLAN を使用していくつかのセグメントに分割し、IEEE802.1x 認証を利用して、機器を適当なセグメントに接続させます。セグメント毎にアクセス制限を設けます（→セキュリティガイドライン：G-3 参照）。

＜アクセスポリシーの例＞

メンバ PC ：すべてのアクセスを許可

その他の PC：制限されたアクセスのみを許可（guest アカウント利用）

その他の機器：内部アクセスのみ許可



その他の IPv6 普及期に向かうための課題（セキュリティ関連除く）

IPv6 サービス提供の基盤

ISP だけでなく、IDC，ホールセラーなどの IPv6 対応が必要です。

アドレスリナンバリング

以下のようなケースでアドレスリナンバリングが発生します。

・ISP との回線接続契約で、IPv4 から IPv4/IPv6 デュアルスタックへ切り替える時
・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替える時

こうした変更のための工数を最小化するための方策を考える必要があります。

各種アプリケーション関連

・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(リバースプロキシ、トランスレータなど)による
・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

検討メンバ

鈴木（日立）
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）
橋本（MRI）
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）

本ガイドラインの改定について

本ガイドラインは、移行 WG によって適宜改定を織り込んでいきます。
これまでの主な変更来歴を下記に示します。

2004/5 月　初版

2005/3 月　改訂版

セキュリティ SWG 発足に伴い下記変更盛り込み。
5 章“セキュリティモデル”の削除
セキュリティに関わる記述部分に対して、セキュリティガイドラインの引用先を追加
2.1 節“IPv6 対応サービス・機器について”の情報更新
2.1 節“IPv6 グローバルアドレスの取得”についての情報追加
2.2 節“新規アプリケーション導入に伴う IPv6 導入”　の内容更新、追加
3 章“独立融合型：　パターン A”　の内容更新
6 章“DNS”　に関する問題点の追加