IPv6移行ガイドライン（案）
（大企業・自治体セグメント）

IPv6普及・高度化推進協議会
移行WG
大企業・自治体SWG

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にを前提に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。

検討メンバ

大企業・自治体SWGメンバ（敬称略）

Co-Chairs

- 月岡（日立）
- 阪内（NEC）

Members

- 荒野（インテックネットコア）
- 伊藤（キャノン）
- 猪俣（富士通）
- 及川（マイクロソフト）
- 太田（NTT東日本）
- 大平（リコー）
- 加藤（NTT）
- 金山（インテックW&G）
- 国武（RINT）
- 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）

目次

1

セグメントの特徴

- 大企業・自治体ネットワークの特徴
- 大企業・自治体ネットワークの分類要素、及びIPv6化との関連性

大企業・自治体ネットワークの特徴

- 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とIPv6化との関連性

(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
- BCPとしてのセキュリティ
- IPv6 ネットワーク構築のフロー
  - 段階置換型の移行パターン
  - 独立融合型の移行パターン
- “今”IPv6を導入する理由

2.1 IPv6ネットワーク環境の先行導入

2.2 新規アプリケーション導入に伴うIPv6導入

2.3 具体的なIPv6導入イメージ

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。
  （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。
  - 既存アプリは既存IPv4ネットワークシステムで継続運用。
  - 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。

＜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。
- 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。
- 定期更新やネットワーク利用ニーズの発生に応じで、徐々にIPv6対応範囲を拡大。

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、“絶対的”なネットワークセキュリティの確保が大前提。 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。

＜緩和モデル＞

⇒現状のF/W設定に、IPv6パケットのforwarding設定を追加することで、IPv6アクセスを部分的に可能にする。

- 第一段階で、一部セグメントをIPv6化。（トンネリング接続）
- 必要なIPv6アクセスについて、F/Wに穴を開ける。
- IPv6の特徴を生かした運用は望めない。

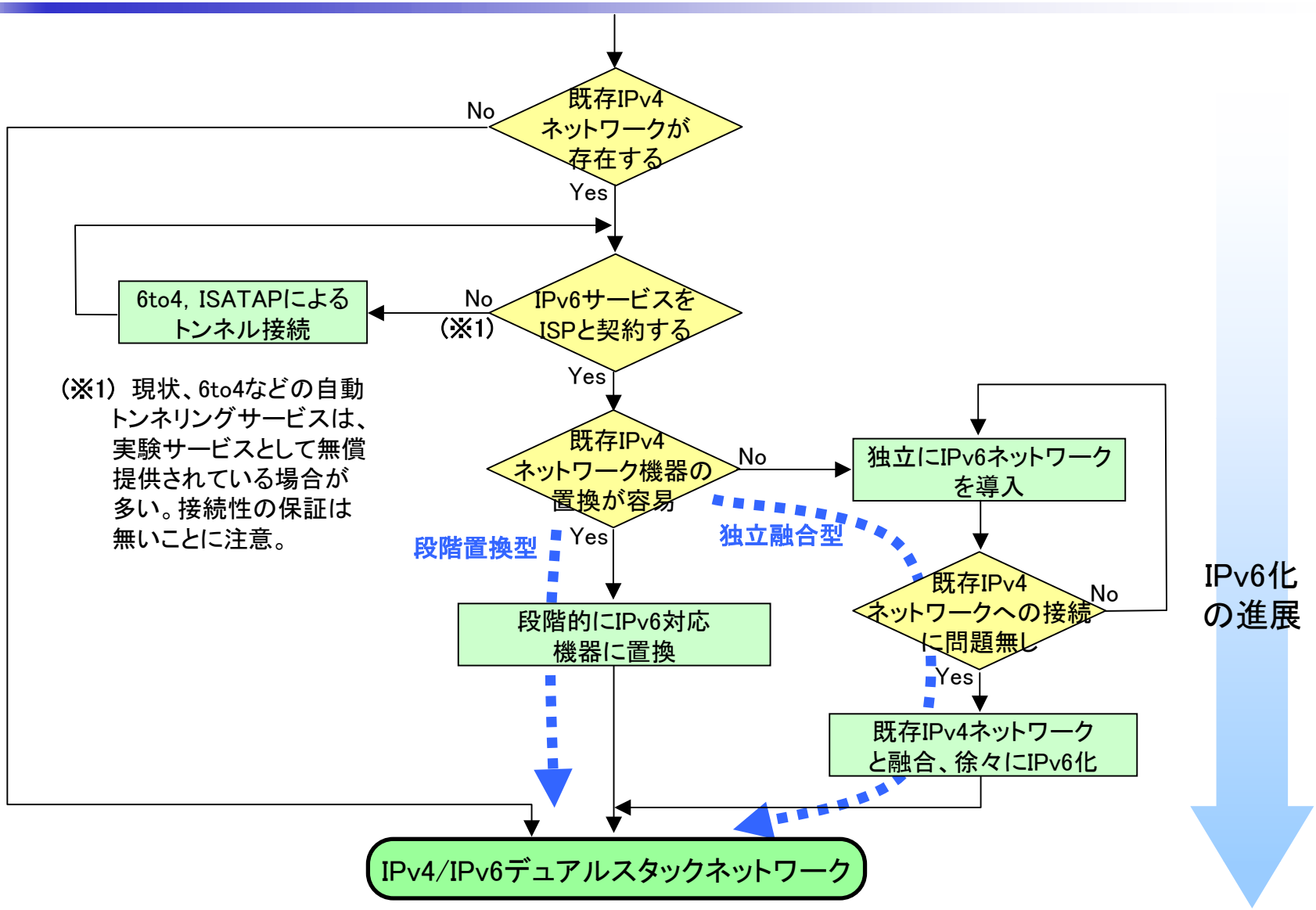
＜厳格モデル＞

⇒現運用ネットワークとIPv6ネットワークの接続を認めない。

- 第一段階で、現用とは独立したIPv6ネットワークを構築。
- セキュリティポリシーが現運用ネットワークと同等以上になるまでは、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、個人情報を取り扱わない。

“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！”

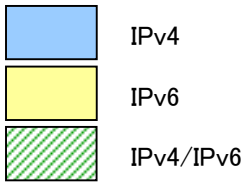
IPv6 ネットワーク構築のフロー

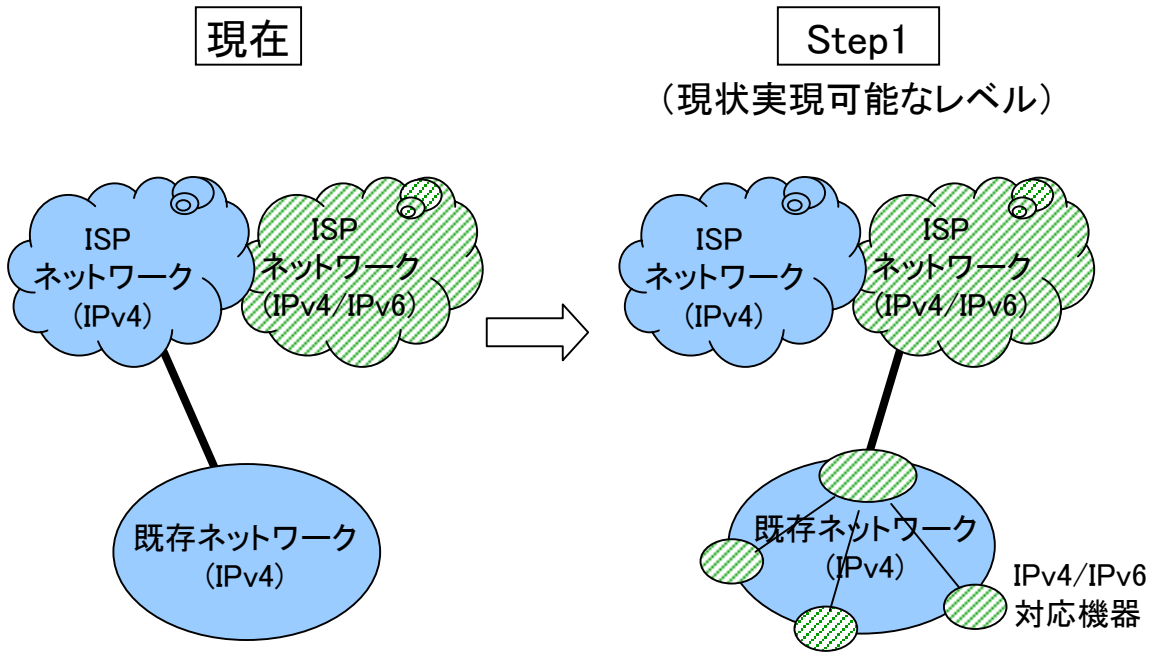


(※1) 現状、6to4などの自動トンネリングサービスは、実験サービスとして無償提供されている場合が多い。接続性の保証は無いことに注意。

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中デュアルスタック対応にする。

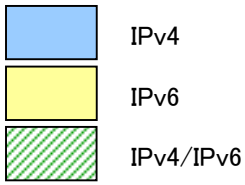


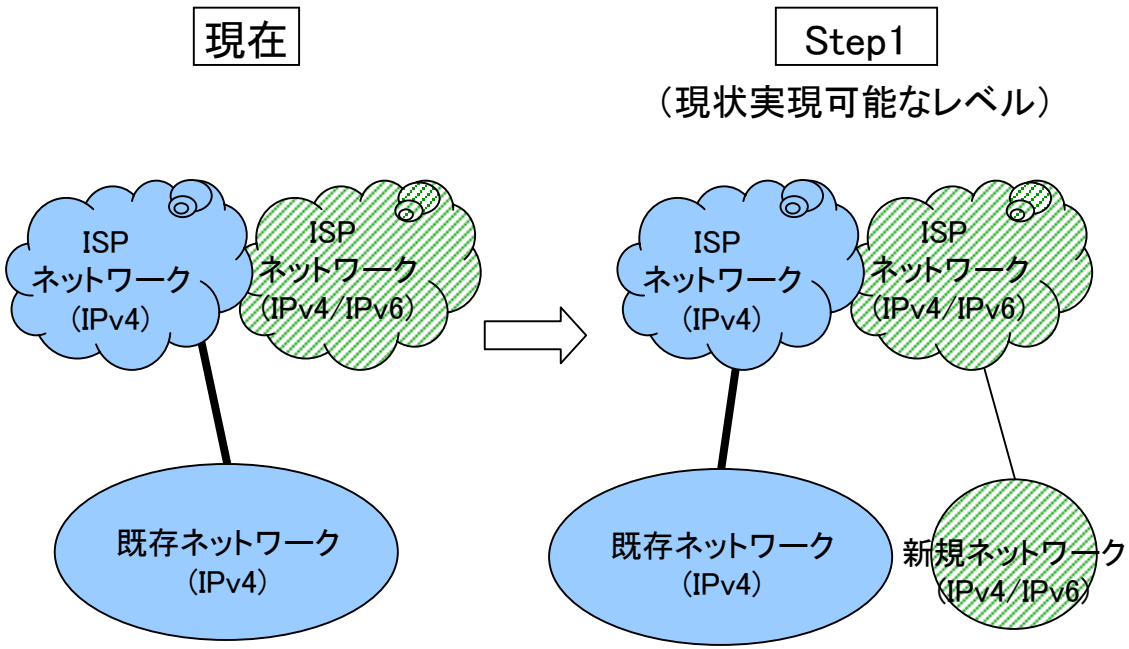


・既存IPv4ネットワークの一部を段階的にIPv6対応機器に置換していく。

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

（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対応のサービス・機器について
- IPv6アドレッシング関連
- ルーティング・トランスレーション・トンネリング
- 境界部分のIPv6化
  - フィルタリング
  - NAT
- DMZのIPv6化
- その他
  - 拠点間接続方式
  - 端末管理

IPv6対応サービス・機器について(1/2)

“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は既に商用サービス開始済。
  （トンネル方式、デュアルスタック方式、ネイティブ方式）
- とりあえずIPv6を体験するならトンネル方式。
  →既存IPv4ネットワークへの影響が最小限。
  但し、カプセリングによるオーバーヘッドは覚悟すべき。
- 本格的なIPv6導入を想定するならデュアルスタック方式。
- いきなりネイティブ回線を利用するのは制約が多い。(DNS、SNMPなど)
  →ネイティブ回線は、主に小規模ISP向けサービス。

＜ルータ＞

- 中～大規模ルータのほとんどは、IPv6対応済。(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い。(RIPng、OSPFv3、PIM-SM)
- 小型ルータのIPv6対応が、意外に遅れている。
- IPv4とは独立のコンフィギュレーション。(ルータのIPv6対応は、今や必須条件!?)

IPv6対応サービス・機器について(2/2)

＜F/W＞

- 基本的なパケットフィルタリング機能がIPv6対応した。
- 機能、性能、信頼性において、検証は必要。
- 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うするか？(今後の課題)
- 現状、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。

＜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。
- 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化まで拘る必要は無い。(AAAAレコード対応が重要)
- 暫定的には、IPv6対応の外部DNSを参照する手も有り？

＜その他サーバ＞

- WebやMail(※1)などは、IPv6対応済み。
- ネットワーク管理サーバは、MIBがIPv6対応。(SNMPはIPv4ベース)

＜PC・PDA＞

- 主要なOSは、ほぼIPv6対応済。(但し、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。
- 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有り。

(※1): MailサーバのIPv6化においては、Virus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。

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＞

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当てを受けることが可能。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当たっては/48のIPv6アドレスを取得することを推奨。

＜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、殆どの大企業・自治体ネットワークにでは、十分なアドレス空間であるが、将来の展開を考慮し、下記の項目に留意すべき。

- シンプルで効率の良い（見易い）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。（※1）
- 対象ネットワークにおける地理的・組織的な構成に合せたアドレス割付け。

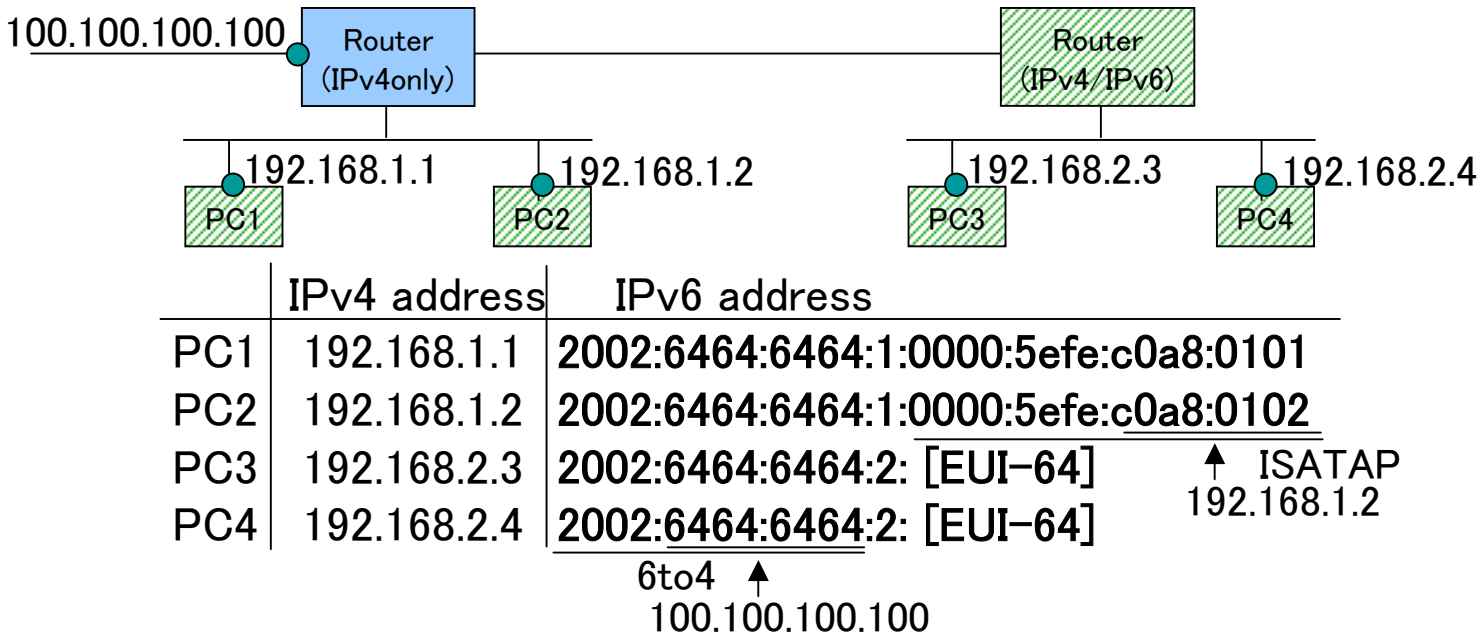
（※1）： IPv6アドレスアサインメントに関する参考情報として、RFC3531が存在。

IPv6 ローカルアドレス付与方法

“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。 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か？

(1) グローバルIPv4アドレスと6to4アドレス生成ルールを利用

（※）：本手法は、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。



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

→ 現在IETFで議論が始まったばかりで、まだ推奨することは出来ない。

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。
- 上位機種では、OSPFv3に対応してるものも有る。
- 他社互換性の検証も実施されており、実用的にも問題無し。

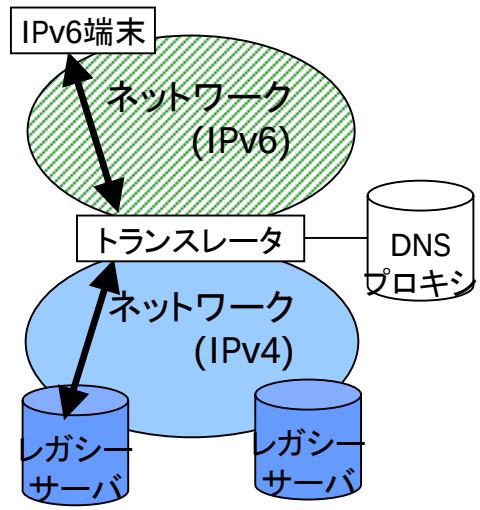
＜大企業・自治体ネットワークにおけるIPv6ルーティングプロトコル＞

- IPv6導入当初は、スタティックルーティングで十分。
- 規模拡大に応じて、RIPng、OSPFv3を導入。
- 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解り易い。
- 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。

トランスレータ

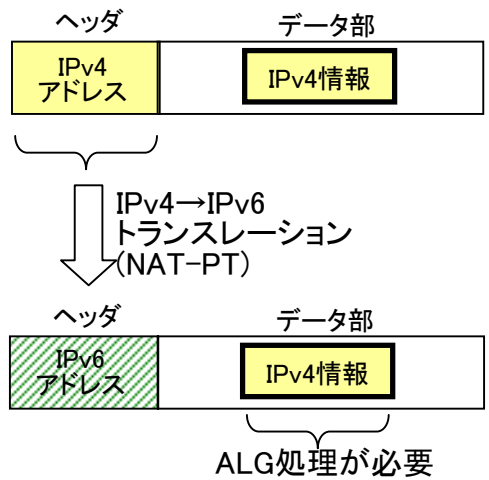
＜特徴＞

- 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。



トンネリング （1/2）

＜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。

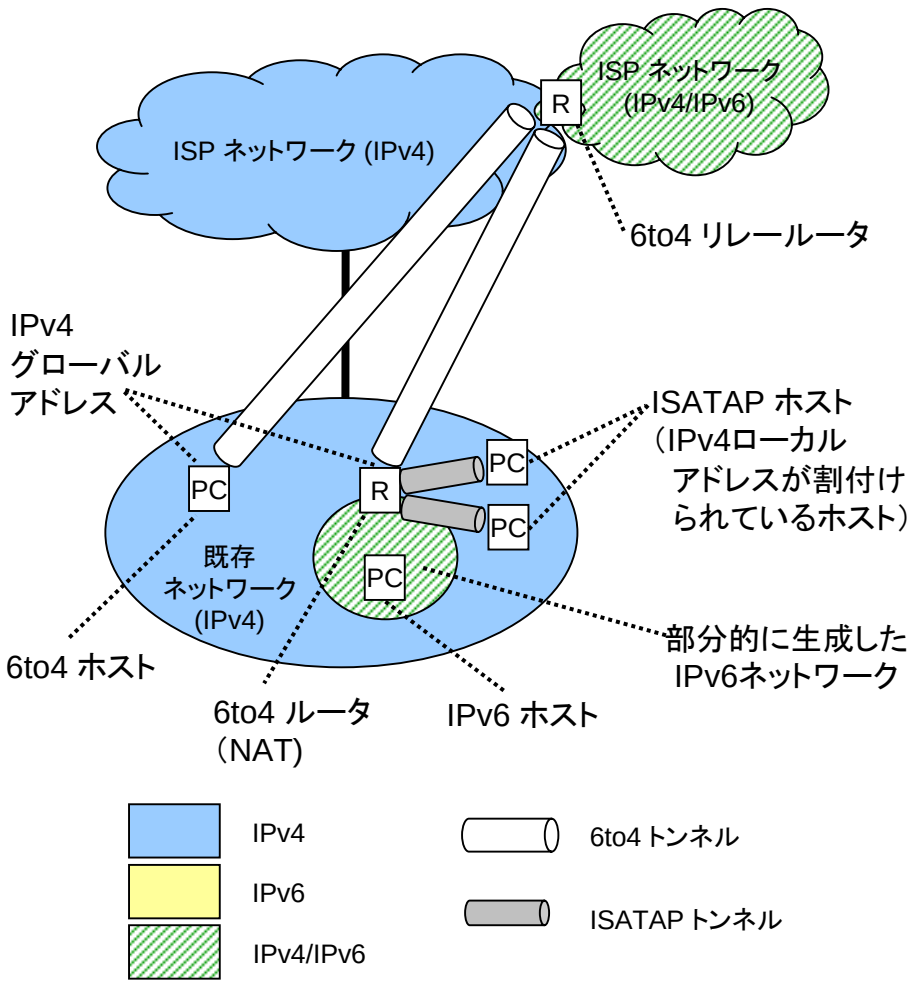
＜自動トンネリング＞

- DTCP（Dynamic Tunneling Control Protocol）
  - クライアント側から動的にトンネル生成を要求可能。
    （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(※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。
  - 往路と復路の経路が同一になる保障が無い。
- 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。
- 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。

(※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。

トンネリング （2/2）

＜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。
- 6to4ルータと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。
- 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。
- 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有る。
- 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無い。

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＞

- ・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

→IPv4では、F/WやNATが上記機能を実現。
（アドレス変換機能以外は、IPv6でも必要。）

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F/W)を追加導入する。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する。

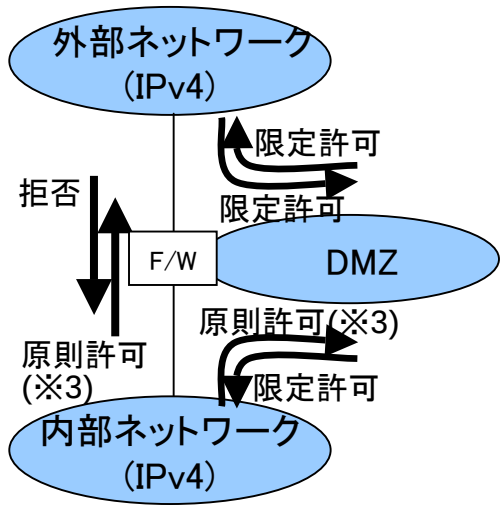
IPv4トラフィックは、既存IPv4部分で処理(※2)する。

(※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

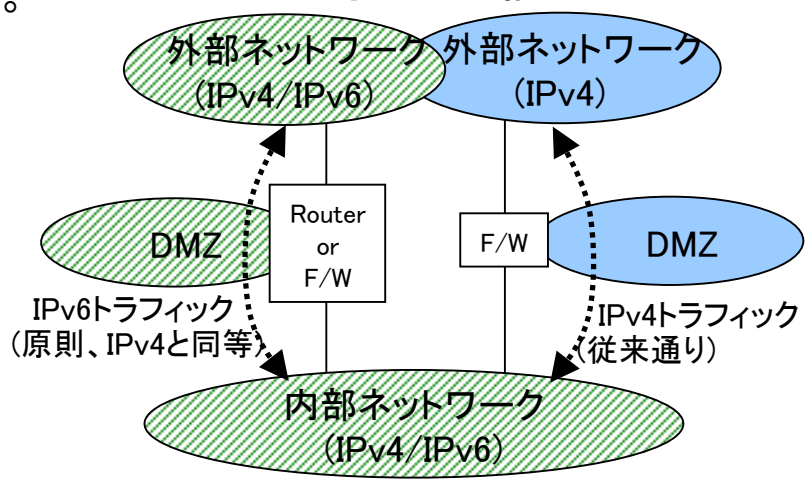
(※2) IPv4/IPv6対応ルータを経由するIPv4トラフィックを処理しない理由は、既存セキュリティレベルのデグレを防ぐこと、及び万一、IPv6側に障害が発生しても既存サービスを継続するためが目的。ロギング、ウィルスチェック、IDS機能においても、同様の考え方。

(※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)とするケースが多い。

＜従来の構成＞



＜IPv6導入時の構成＞

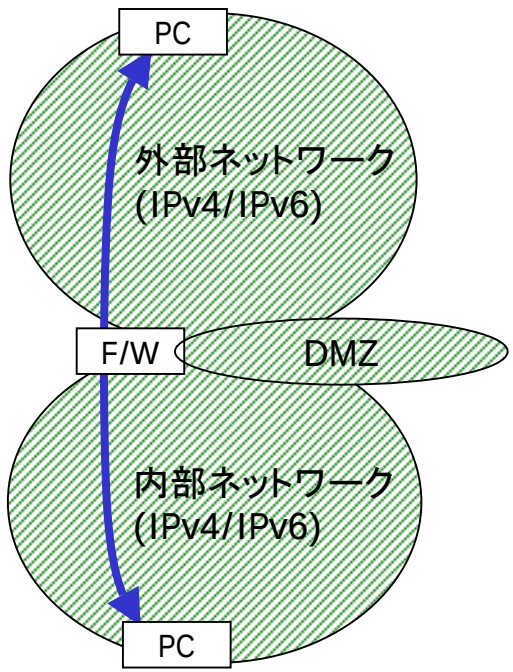


フィルタリング（1） ～IPv6対応F/Wの場合～

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＞

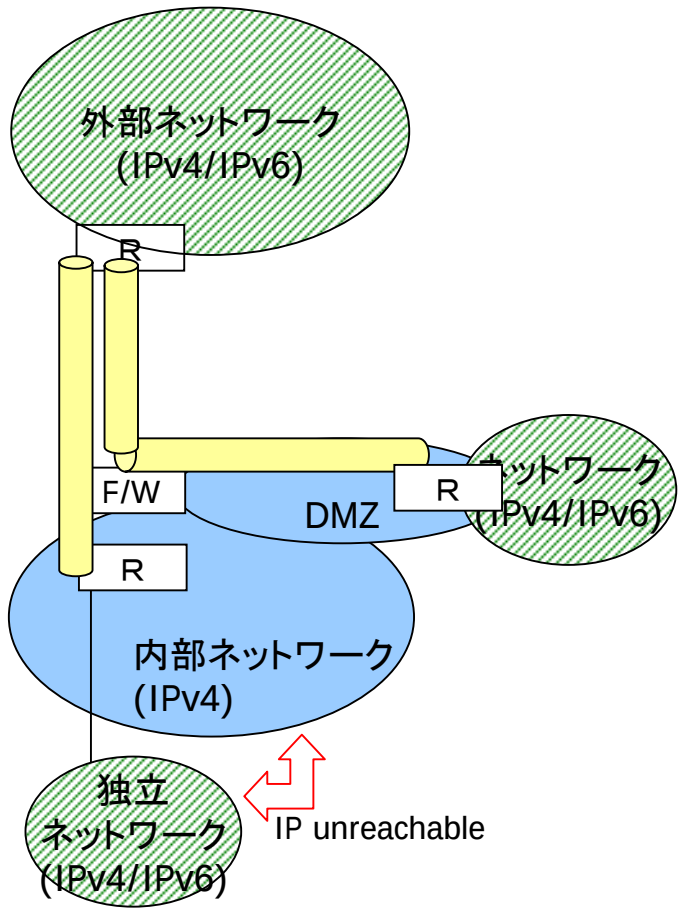
- F/Wを経由するE2E通信を許容する場合、限定した端末において特定のアクセス(IPアドレス、ポート番号でフィルタリング)のみを通過させるべき。
- F/Wを経由するIPsecベースのE2E通信は、今後の課題。（試験的に許容する場合は、限定した端末において特定のアクセス(IPアドレスでフィルタリング)のみを通過させるべき。その際、終端装置には、パーソナルF/Wなどのセキュリティ対策を導入すべき。）



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＞

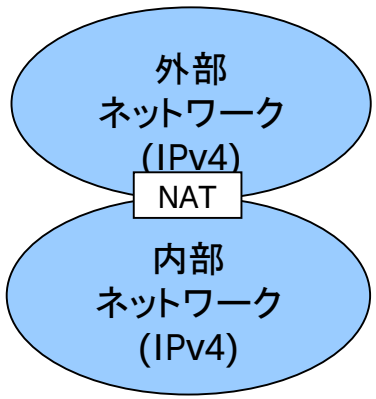
- 基本は、IPv6overIPv4トンネリングアクセスをDMZ向けに対して許可（IPプロトコル番号41の通過を許可）し、DMZにおける部分的なIPv6対応セグメントを生成する。
- IPv6overIPv4トンネル通信を内部ネットワークへ許可（IPプロトコル番号41を通過）する場合は、当面は既存ネットワークとは独立したネットワーク（IP unreachable）で試行すべき。



NAT

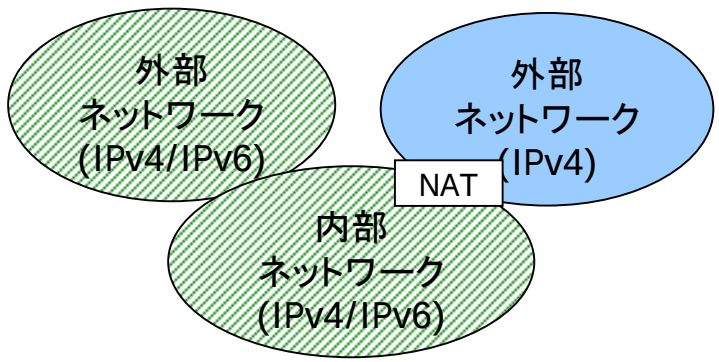
- IPv4では、アドレス空間節約の為、NATを多用(※1)していた。
- **IPv6では、原則としてNATを用いたローカルアドレスは使用しない。**

＜従来の構成＞



IPv4： ローカルアドレス

＜IPv6導入時の構成＞



IPv6： **グローバルアドレス**
IPv4： ローカルアドレス

＜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だった。アドレス情報秘匿(※2)の必要性については、今後の課題である。

(※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)する例も有る。
(※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。

リモートアクセス

＜現状のリモートアクセス方式＞

(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でアクセス

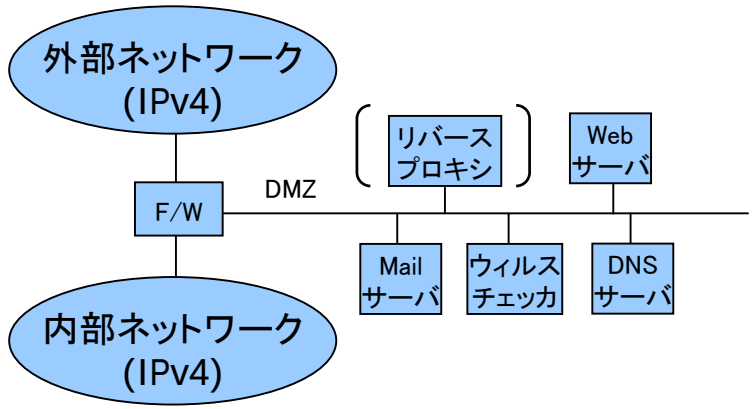
(c) インターネットVPN(トンネルモード)

(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。但し、”IPv6 over IPv4 over IPv4(セキュリティトンネル)” となる為、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る。

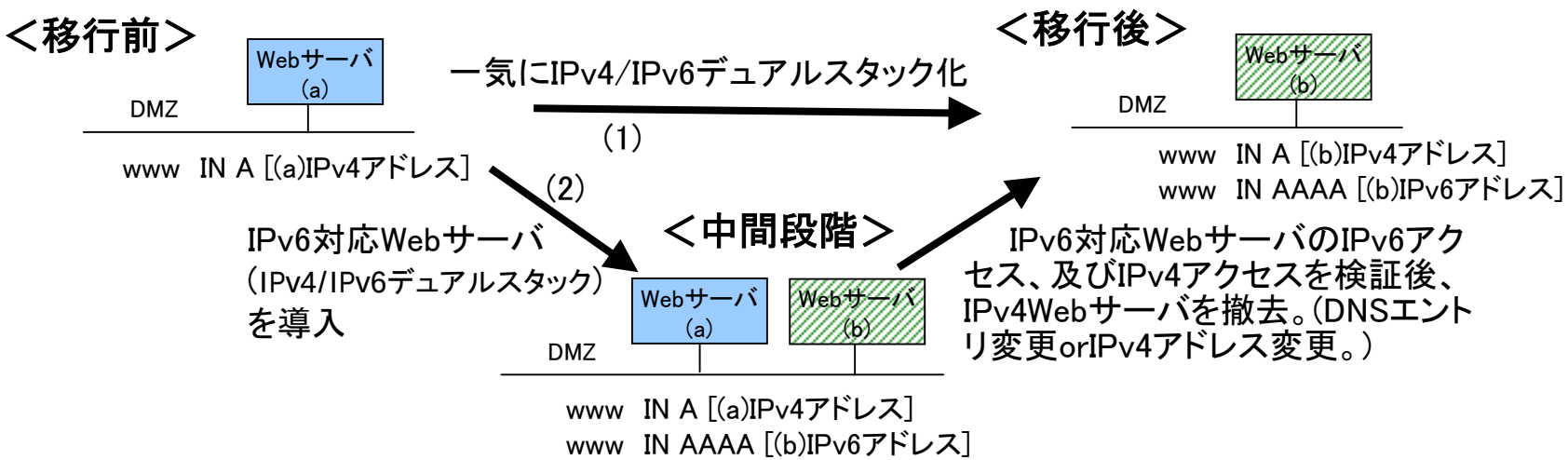
DMZのIPv6化： Webサーバ

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、右記に示す。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る。



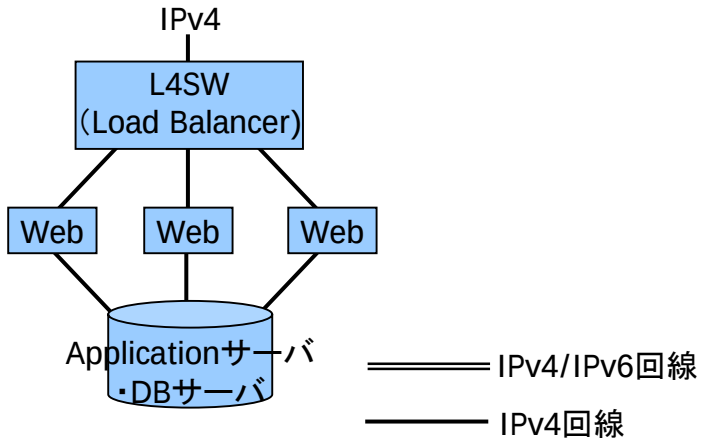
＜WebサーバのIPv6化＞

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。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る。



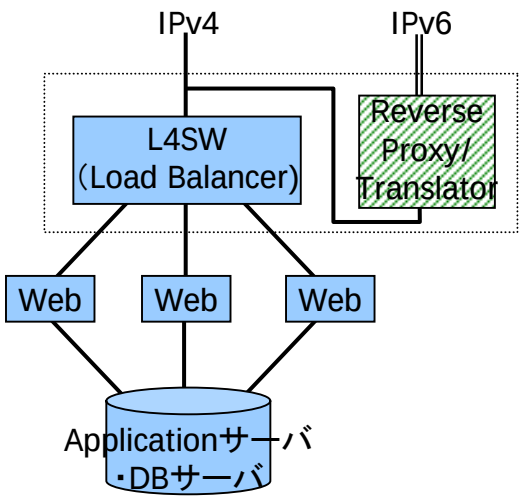
WebサーバのIPv6化： 大規模システムの場合

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右記に示す。
IPv6移行に当たって、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る。



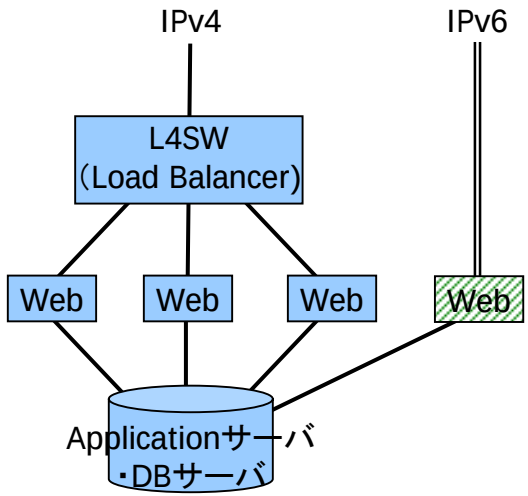
＜構成1＞

IPv6ベースのアクセスは、Reverse Proxyにてプロトコル変換し、既存のIPv4ベースのアクセスと同等の扱いで処理する。



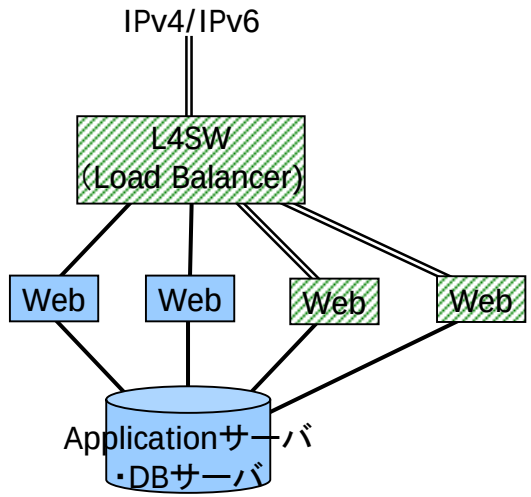
＜構成2＞

IPv6ベースのアクセスは、負荷分散処理せず、個別にIPv6対応のWebサーバを設置する。



＜構成3＞

L4SW、及びWebサーバをIPv6対応させる。



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。

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、Privacy Extensionは使用しないことが前提。)

(※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。)

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
- VoIPv6ソリューション
  - 現状のIP電話導入パターン
  - IPv4によるIP電話の拡張（外線接続）
  - VoIPv6ソリューション　～大規模拠点向け～
  - VoIPv6ソリューション　～小規模拠点向け～
  - VoIPv6ソリューション　～もう1つのメリット～

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、Virus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？

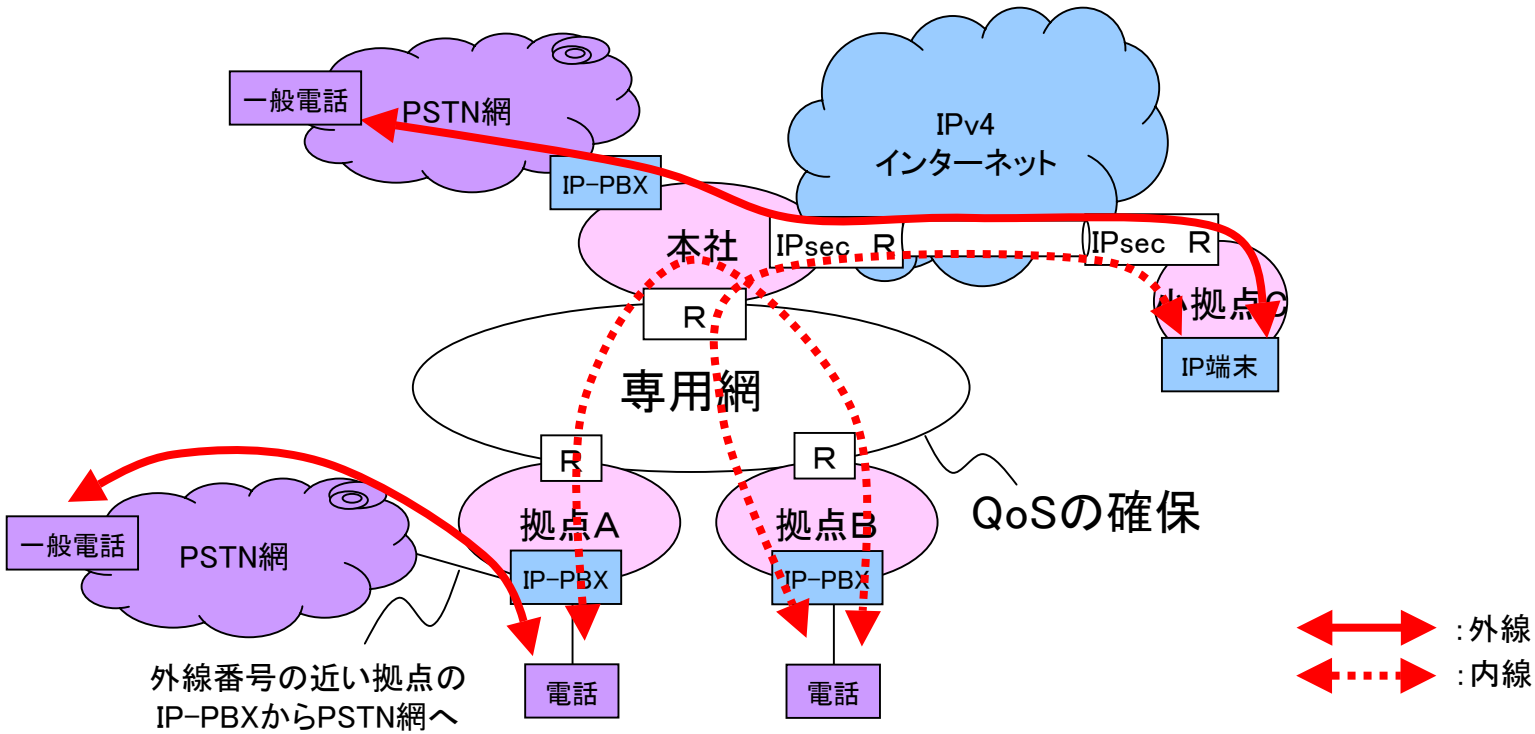
P2Pアプリケーション	イントラ内	外部(特定)	外部(不特定)
VoIP	○	○	○
IM(インスタントメッセンジャ)	○	○	○
グループウェア	○	○	―
サーバレス ファイル共有	○	○	―
メンテナンス／モニタリング	○	○	―
マルチキャストストリーミング	○	―	―
固定アドレス(MIP)	○	○	―
テレビ会議	○	○	―

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。
- IPv6契約をして必要なトラフィック用にF/Wに穴を開けるのみ。
- 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。
  - 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）
- 当面、F/W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。
- 実際の導入に際しては、各企業のセキュリティポリシにより、独立融合型，段階置換型を選択。
- 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、〇〇ソリューションとして、同じ論理で構築が可能。

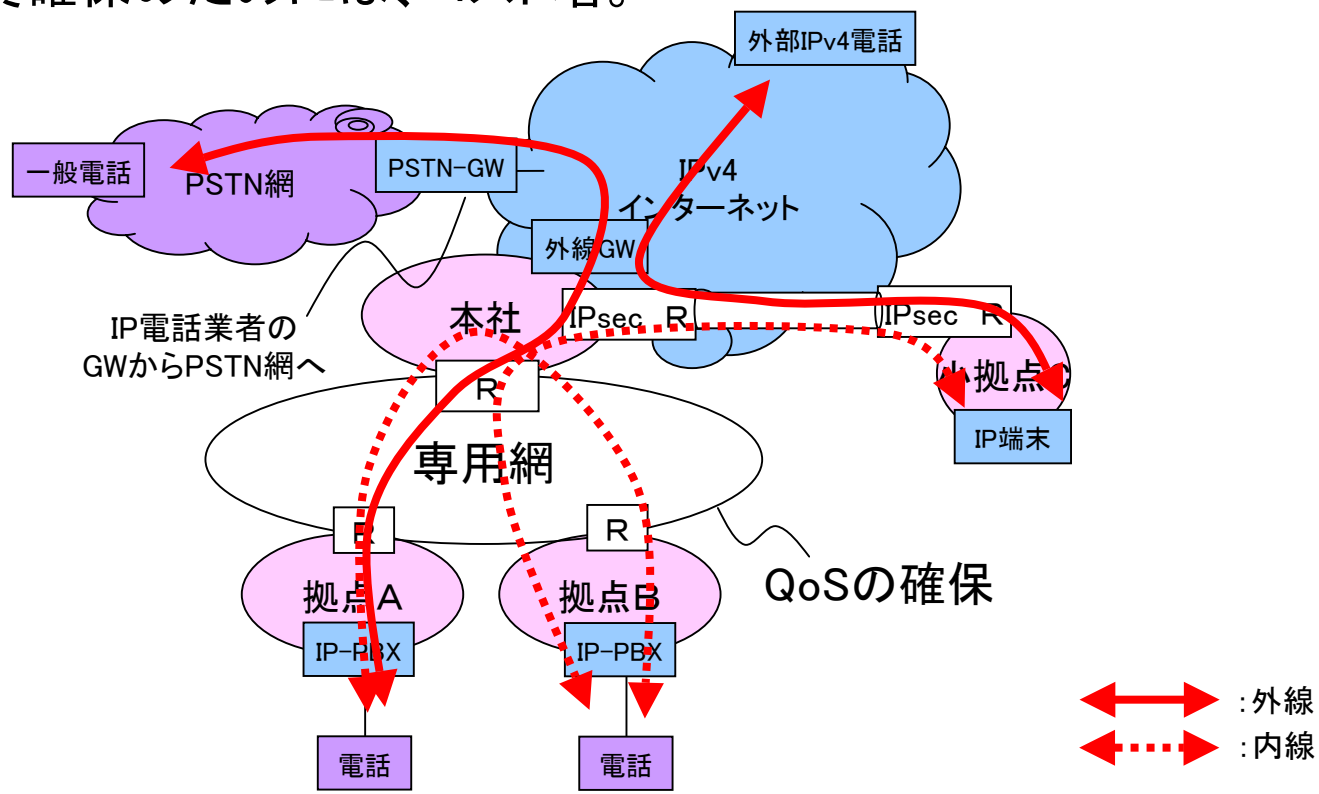
現状のIP電話導入パターン

- 主に内線電話に利用。
  - 外線のIP電話接続はこれから。
- 大規模拠点は、QoS確保のため専用線相当の接続。
- 小規模拠点は、インタネットVPNで接続。
  - 問題点：小規模拠点向けの通信トラフィックの複雑化。



IPv4によるIP電話の拡張（外線接続）

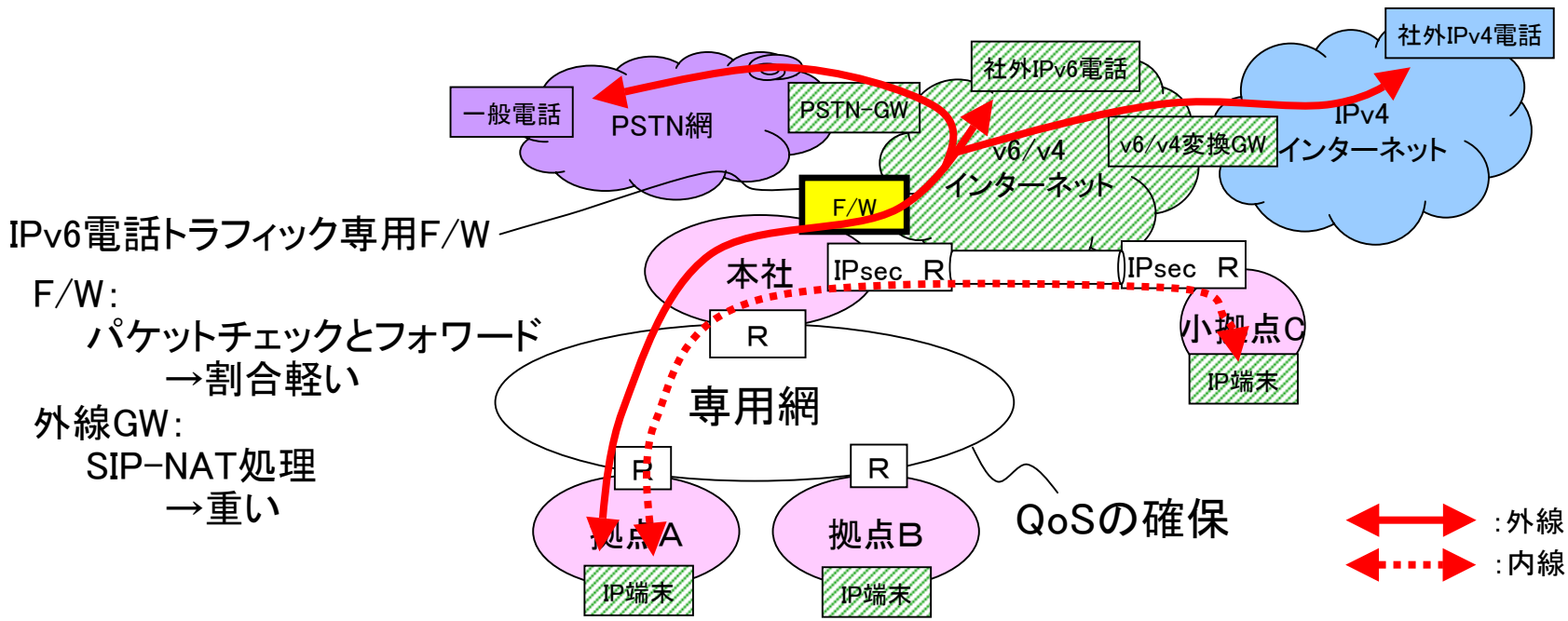
- 外部のIP電話との接続に、外線GW（SIP-NAT）は必須。
- すべての外線トラフィックは、外線GW経由。（PSTNコールも）
- 外線需要に合わせた外線GWの容量確保が必須。
  →通話品質確保のためには、コスト増。



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GWの負荷を軽減。
  “IPv6外線は、外線GWを通らない” →F/Wを通る。
  - 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:
  - 本社・外線GWの負荷軽減→コスト削減。

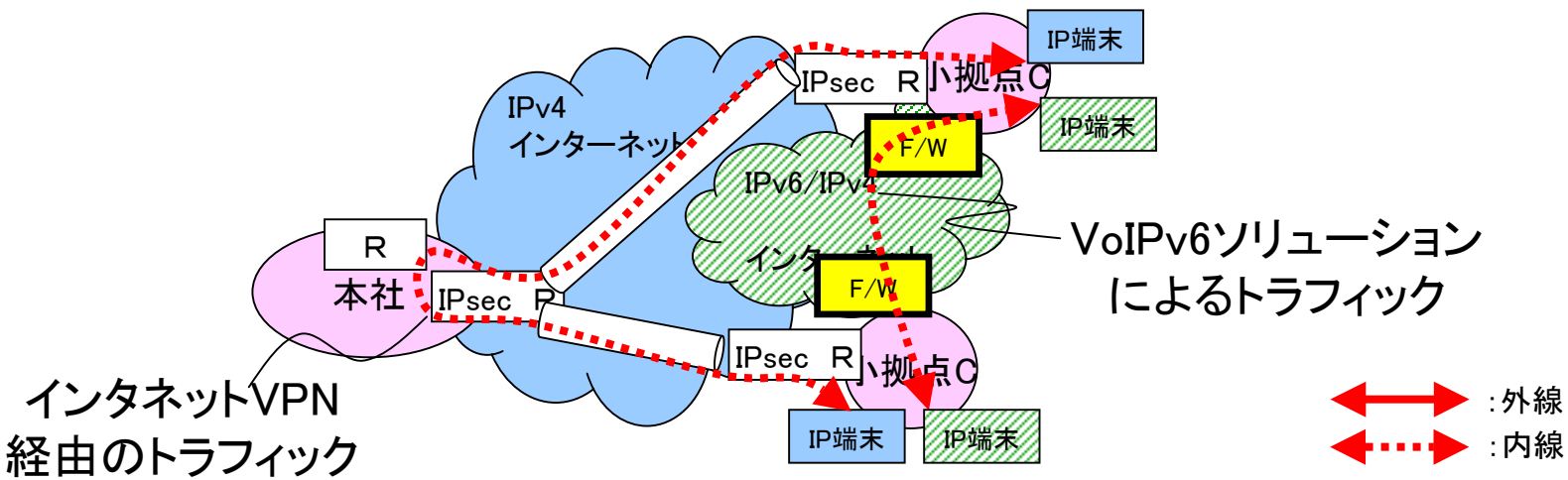


VoIPv6ソリューション　～小規模拠点向け～

- 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。



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。
  - 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。
  - サブネットマスクを変更する。

  or
  - 別セグメントを追加する（＝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大。

- IPv6ならば、IPv4で必要とされる再設計は不要。

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例： パターンA
  - 段階置換型
  - 独立融合型
- 大企業・自治体ネットワークの例： パターンB
  - 段階置換型
  - 独立融合型

大企業・自治体ネットワークの分類要素： パターンA

(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

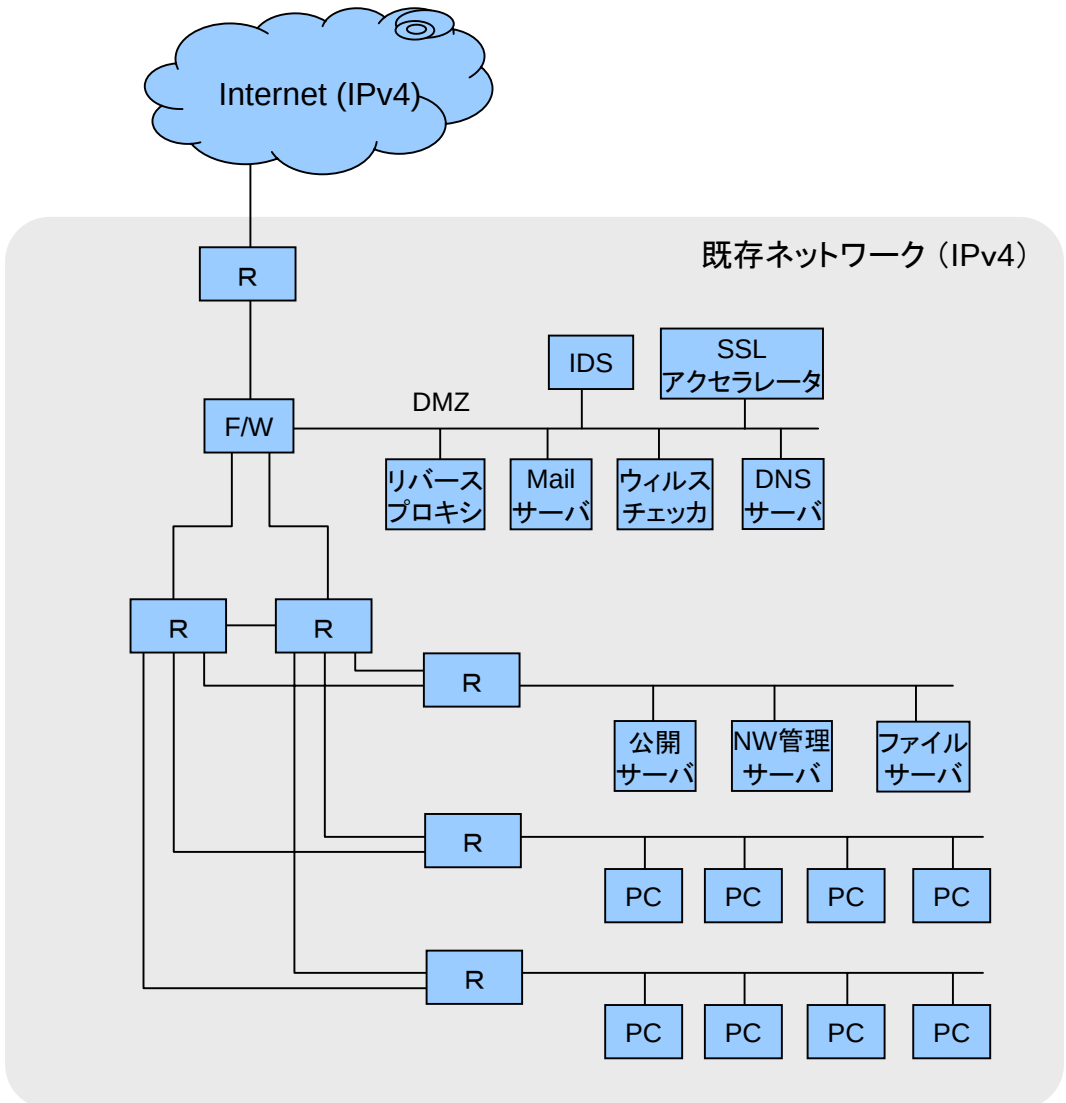
(7) 冗長構成（ISP接続回線、基幹装置など）
- ■ 有り
- ■ 無し

(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

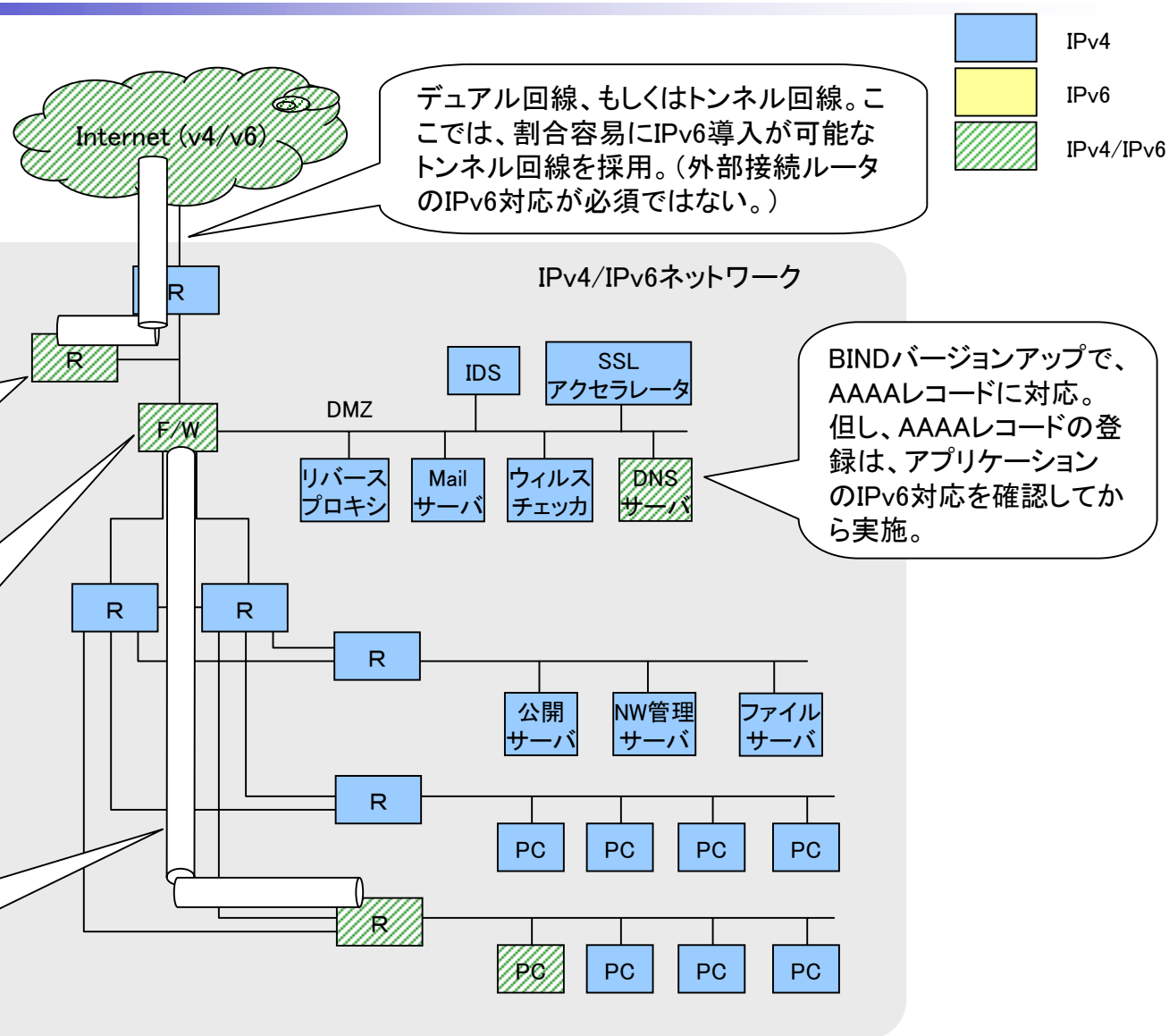
(10) VoIPの導入
- ■ 有り
- ■ 無し

大企業・自治体ネットワークの例： パターンA

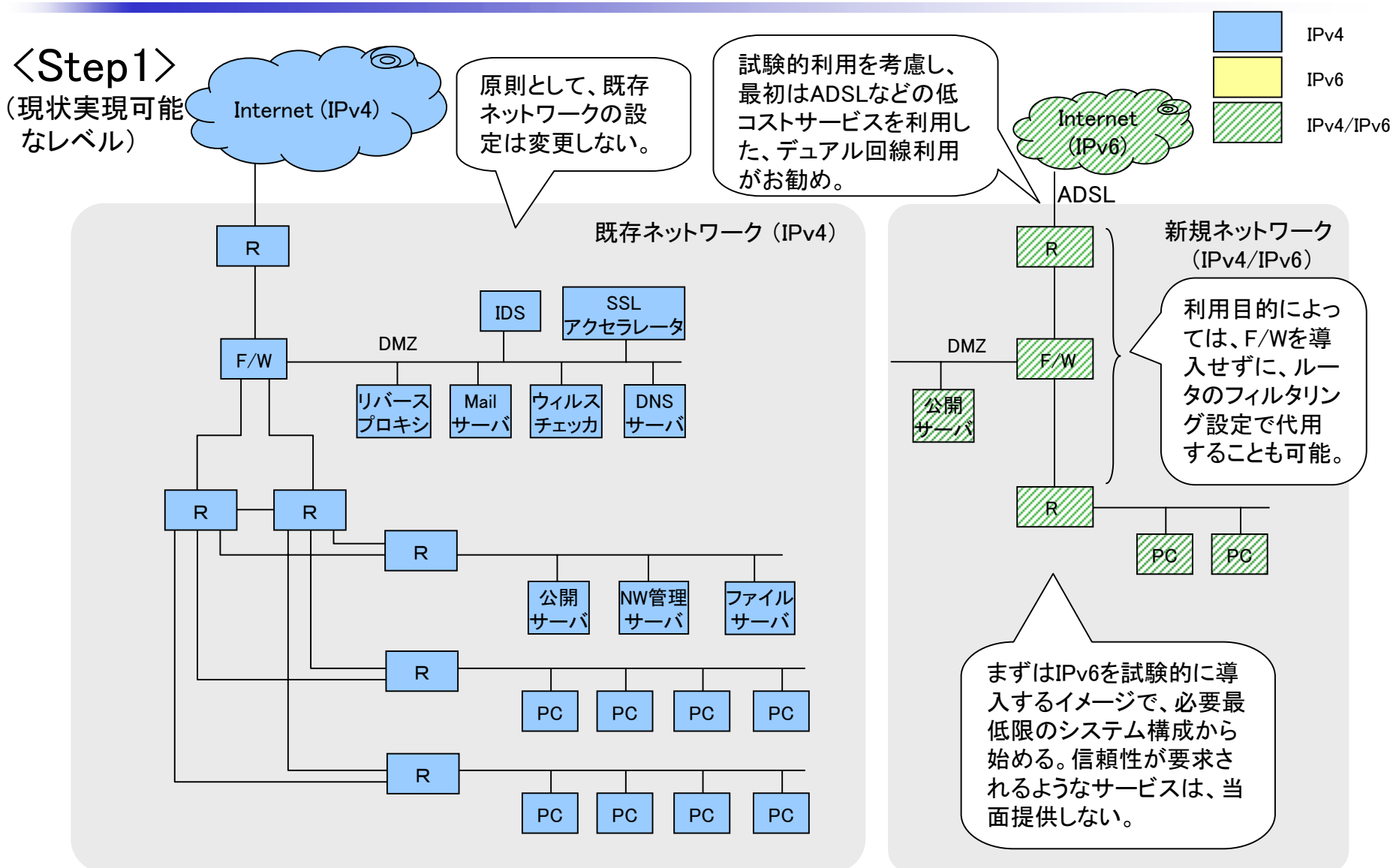


段階置換型： パターンA

〈Step1〉
（現状実現可能なレベル）



独立融合型： パターンA


〈Step1〉
（現状実現可能なレベル）
Internet（IPv4）
原則として、既存ネットワークの設定は変更しない。
試験的利用を考慮し、最初はADSLなどの低コストサービスを利用した、デュアル回線利用がお勧め。
Internet（IPv6）
IPv4
IPv6
IPv4/IPv6
ADSL
既存ネットワーク（IPv4）
新規ネットワーク（IPv4/IPv6）
R
F/W
DMZ
IDS
SSL アクセラレータ
リバースプロキシ
Mail サーバ
ウィルスチェッカ
DNS サーバ
公開サーバ
NW管理サーバ
ファイルサーバ
PC
利用目的によっては、F/W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。
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。信頼性が要求されるようなサービスは、当面提供しない。

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

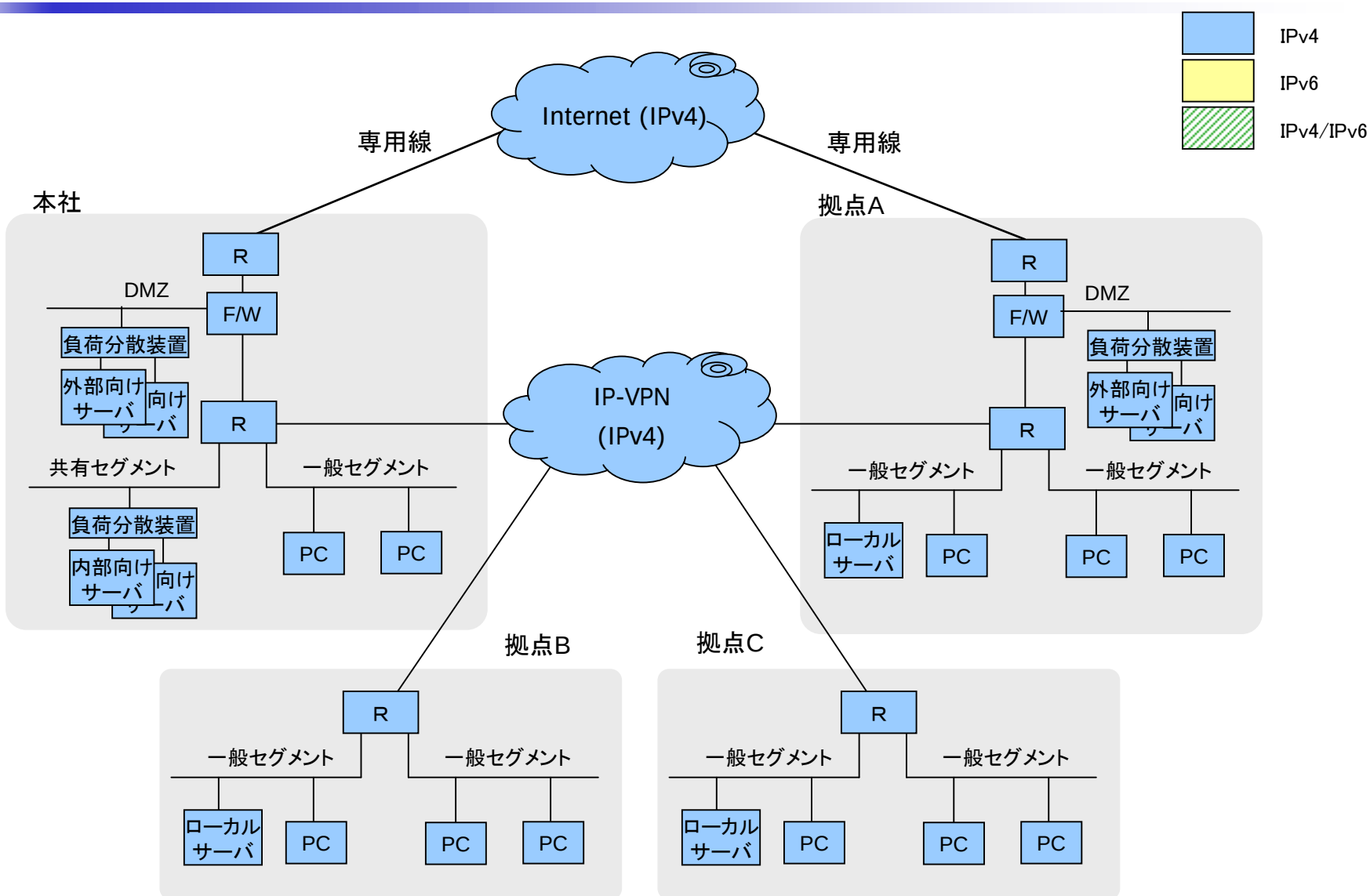
(7) 冗長構成（ISP接続回線、基幹装置など）
- 有り
- ■ 無し

(8) リモートアクセス
- 有り
- ■ 無し

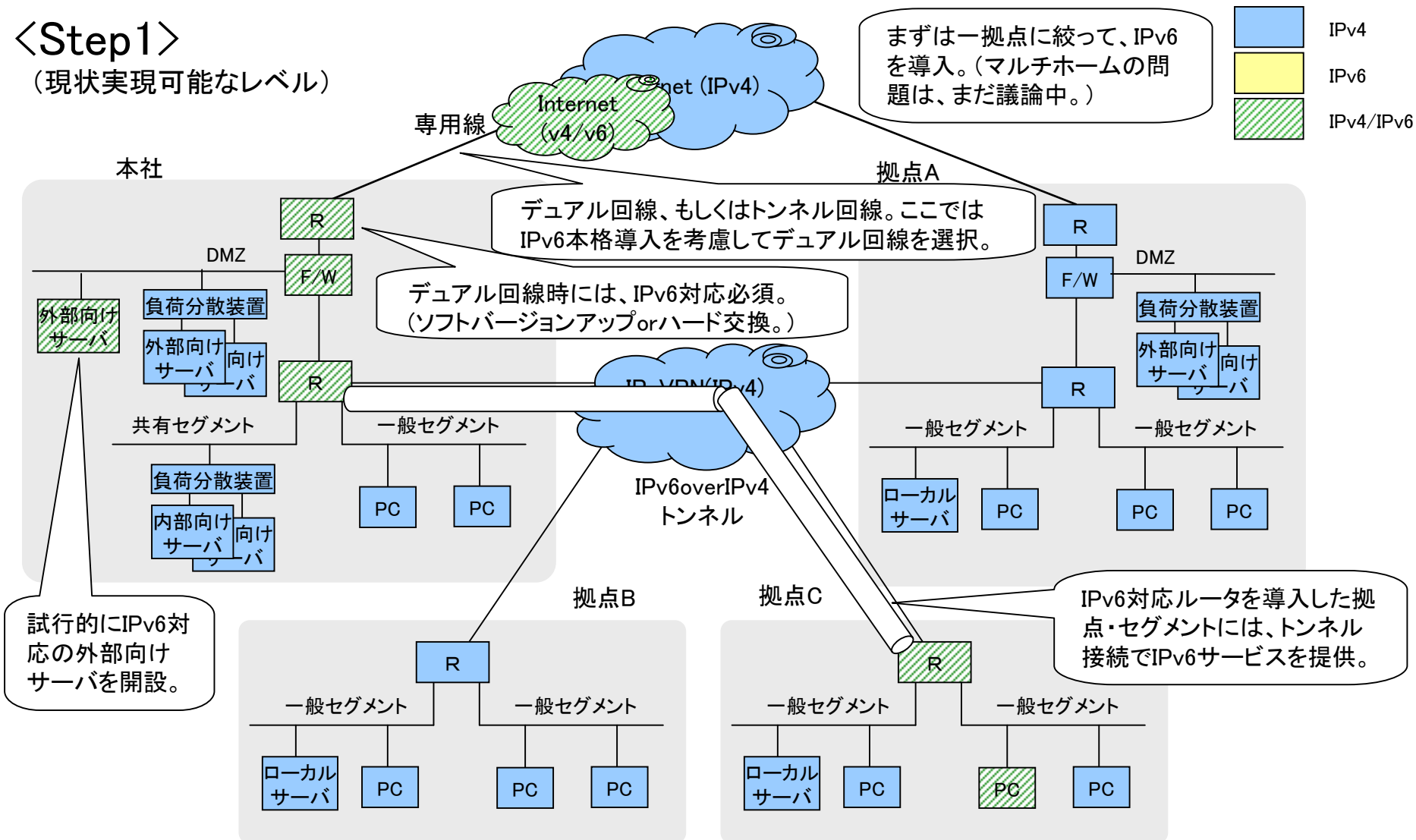
(9) アドレス運用
- グローバル
- ■ プライベート

(10) VoIPの導入
- 有り
- ■ 無し

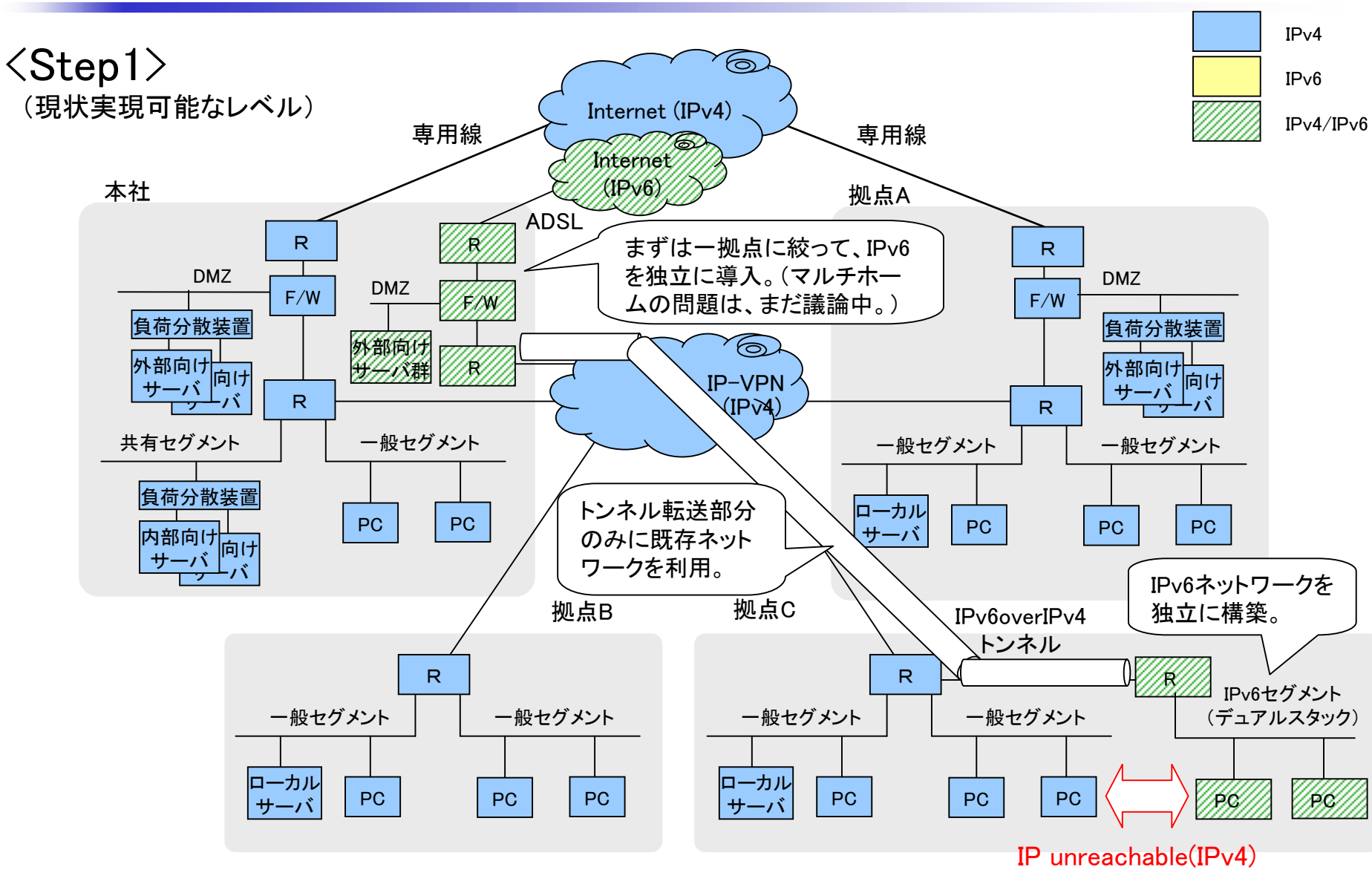
大企業・自治体ネットワークの例： パターンB



段階置換型： パターンB


〈Step1〉
（現状実現可能なレベル）
IPv4
IPv6
IPv4/IPv6
まずは一拠点に絞って、IPv6を導入。（マルチホームの問題は、まだ議論中。）
Internet (IPv4)
Internet
(v4/v6)
専用線
本社
拠点A
拠点B
拠点C
R
F/W
DMZ
外部向けサーバ
負荷分散装置
内部向けサーバ
共有セグメント
一般セグメント
PC
ローカルサーバ
デュアル回線、もしくはトンネル回線。ここではIPv6本格導入を考慮してデュアル回線を選択。
デュアル回線時には、IPv6対応必須。
（ソフトバージョンアップorハード交換。）
IPv6overIPv4
トンネル
試行的にIPv6対応の外部向けサーバを開設。
IPv6対応ルータを導入した拠点・セグメントには、トンネル接続でIPv6サービスを提供。

独立融合型： パターンB


〈Step1〉
（現状実現可能なレベル）
IPv4
IPv6
IPv4/IPv6
Internet (IPv4)
Internet (IPv6)
専用線
専用線
本社
拠点A
ADSL
まずは一拠点に絞って、IPv6を独立に導入。（マルチホームの問題は、まだ議論中。）
R
F/W
DMZ
負荷分散装置
外部向けサーバ
向けサーバ
外部向けサーバ群
IP-VPN (IPv4)
共有セグメント
一般セグメント
PC
ローカルサーバ
トンネル転送部分のみに既存ネットワークを利用。
拠点B
拠点C
IPv6overIPv4トンネル
IPv6ネットワークを独立に構築。
IPv6セグメント（デュアルスタック）
IP unreachable(IPv4)

3

5:5のときの目標とするNW＆システム形態＋アプリケーション

- 5:5段階において想定されるIPv6利用環境と基本方針
- 段階置換型
  - 移行パターン
  - パターンA
  - パターンB
- 独立融合型の
  - イメージ移行パターン
  - パターンA
  - パターンB
- アプリケーション：IPv6で実現したいこと

5:5段階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＞

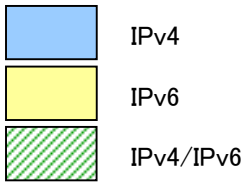
- IPv6ネットワーク環境の充実。
  - 中小規模ISPによるIPv6回線サービス。（デュアルスタック、トンネル）
  - 大型～小型ルータの製品バリエーション充実。
  - 基本OSのIPv6機能本格対応。（モバイル、IPsec、）
  - 各種IPv6対応アプリケーションソフトが普及。
  - ファイアウォール、IDSなどのセキュリティ対策製品の充実。
- 新しいネットワークの枠組みの普及。
  - non-PCのネットワーク接続。（ユビキタス化の進展）
  - 組織単位のセキュリティ管理から個人単位のセキュリティ管理へ。
- IPv4/IPv6デュアル環境でのセキュリティポリシーが確立。
  - 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?

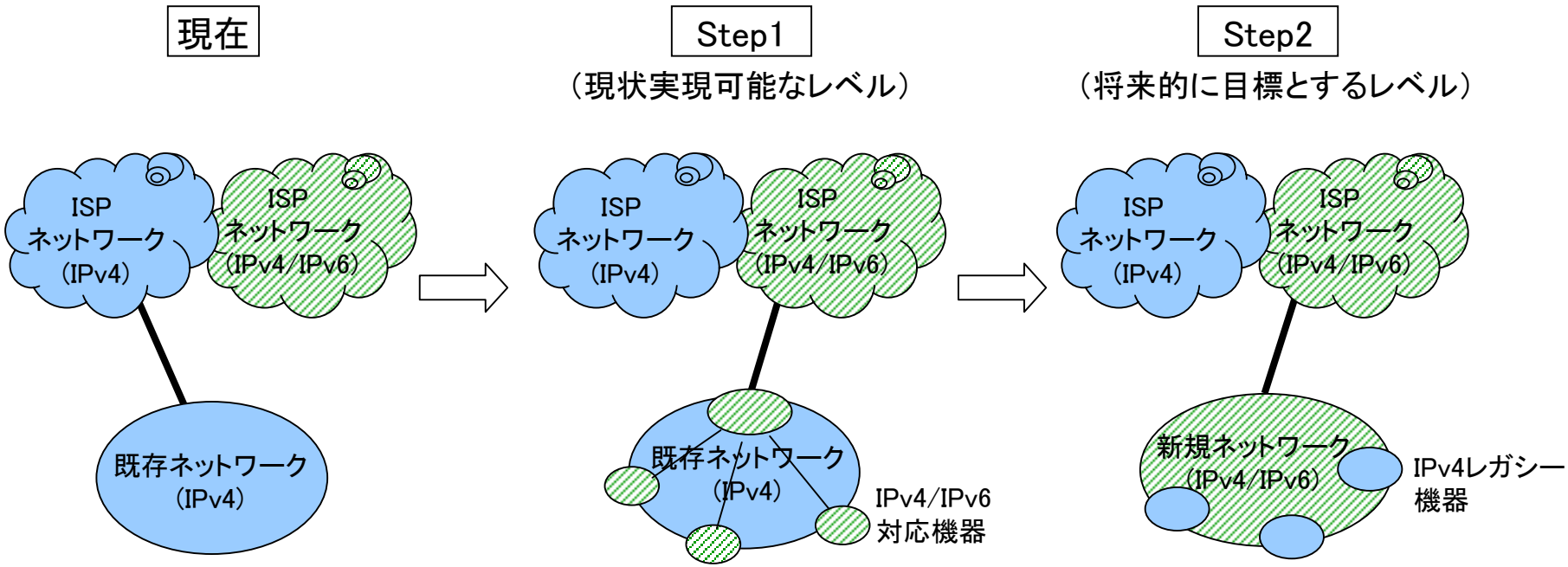
＜基本方針＞

- 全面的にIPv4/IPv6デュアルスタックネットワーク環境を導入。
- IPv6中心のアプリケーション利用環境へ順次シフト。（レガシーアプリは、無理にIPv6対応させる必要は無い。）

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中デュアルスタック対応にする。



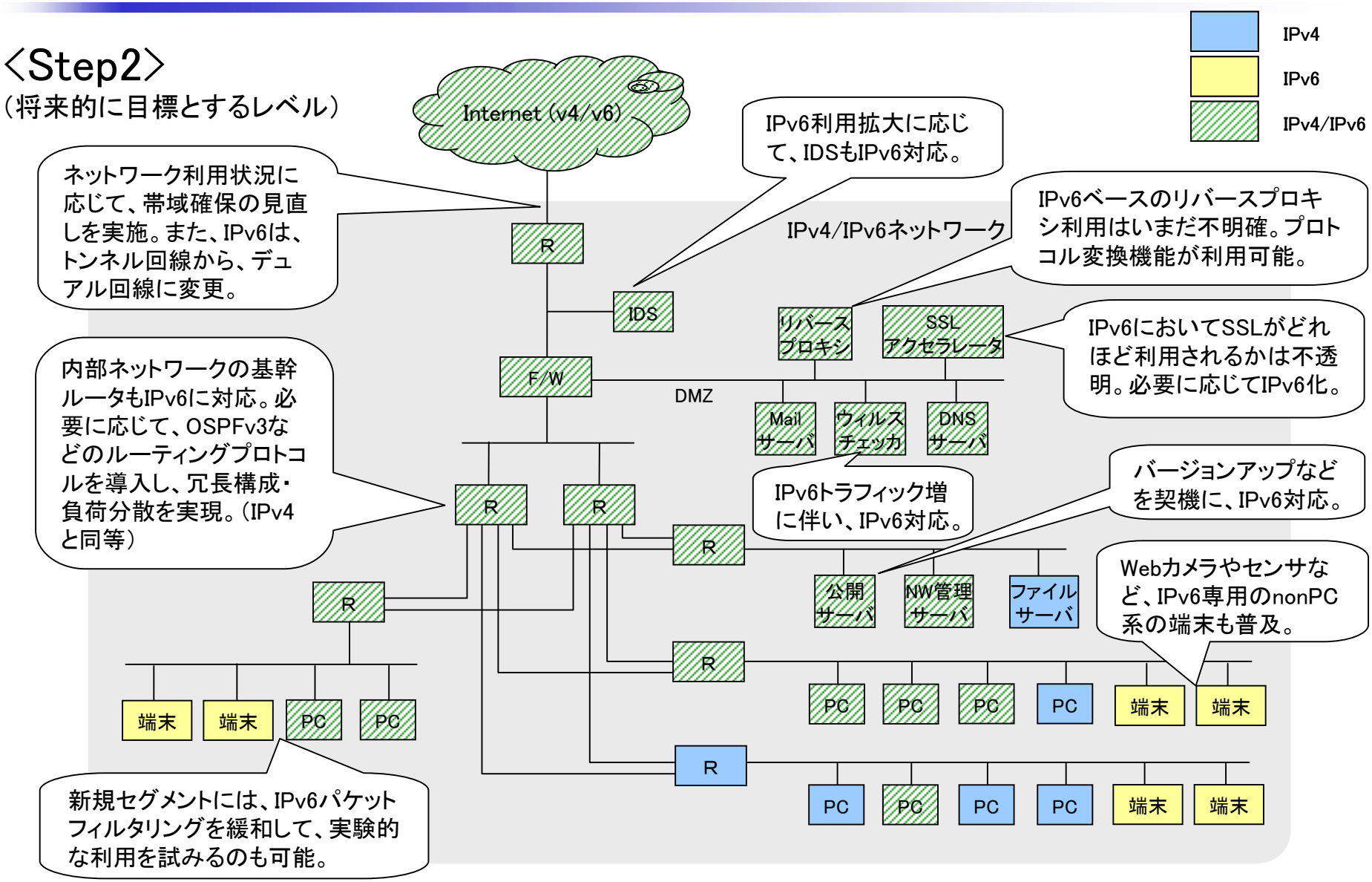


・既存IPv4ネットワークの
一部を段階的にIPv6対応
機器に置換していく。

・IPv4からIPv6へ移行の進展。
・IPv4レガシー設備が残存。

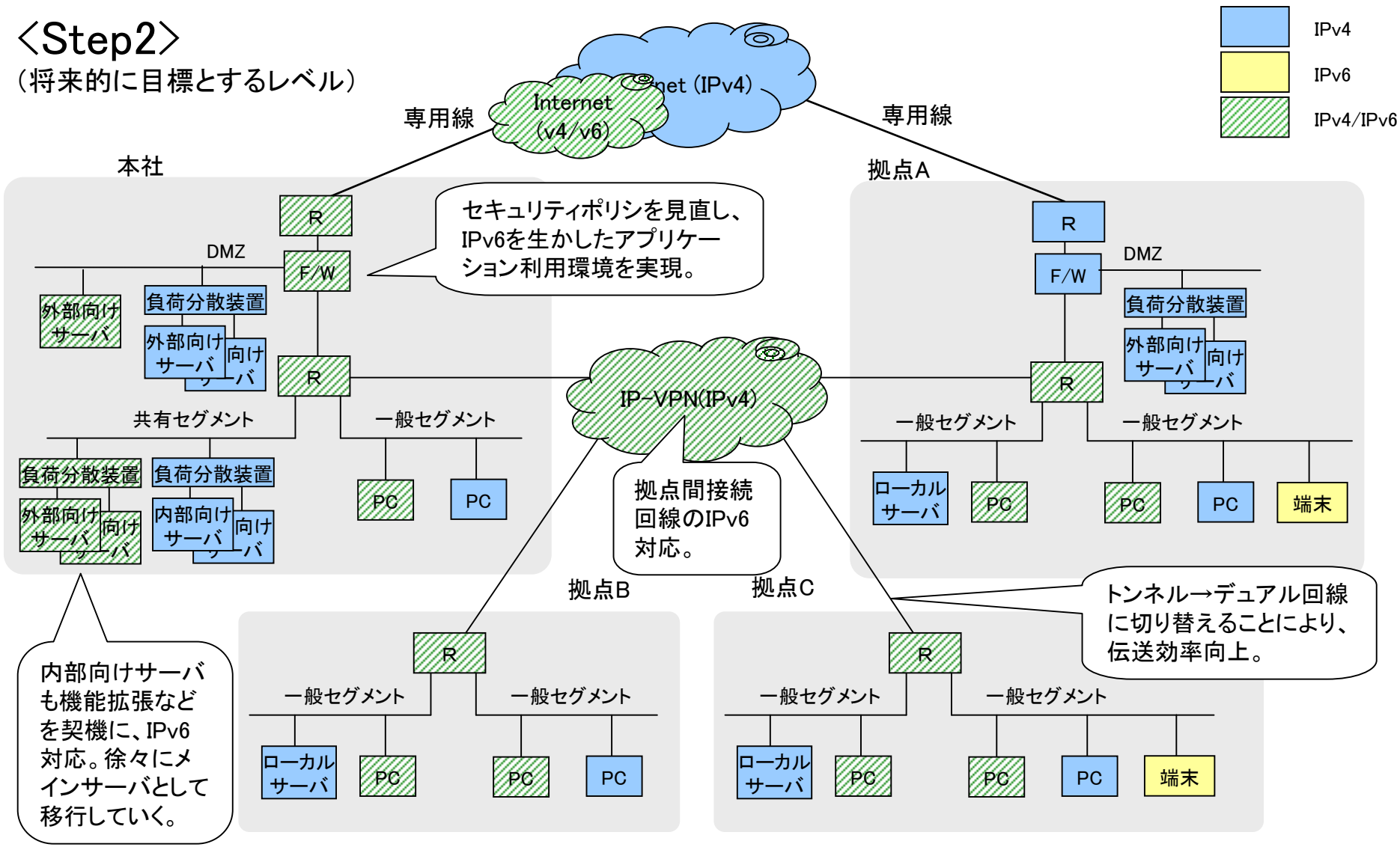
段階置換型： パターンA

〈Step2〉
（将来的に目標とするレベル）



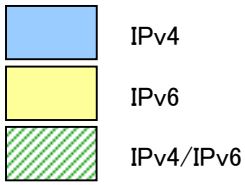
段階置換型： パターンB

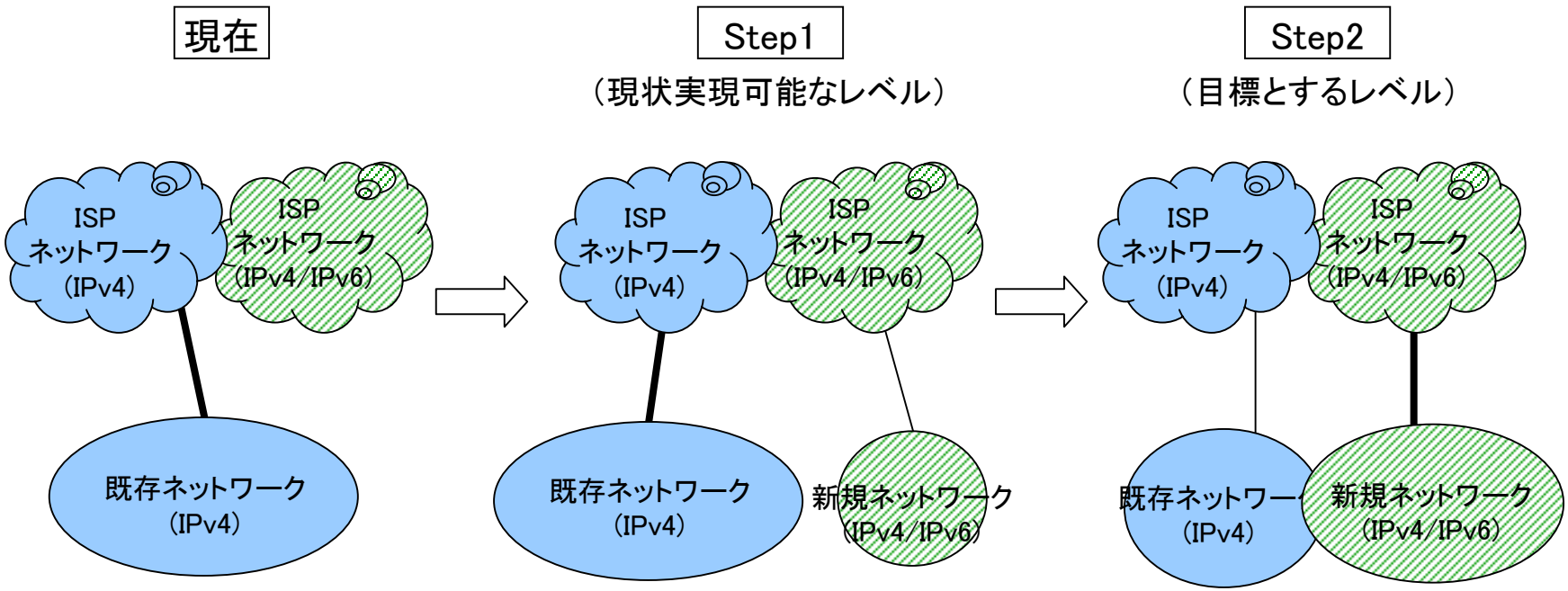
〈Step2〉
（将来的に目標とするレベル）



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。



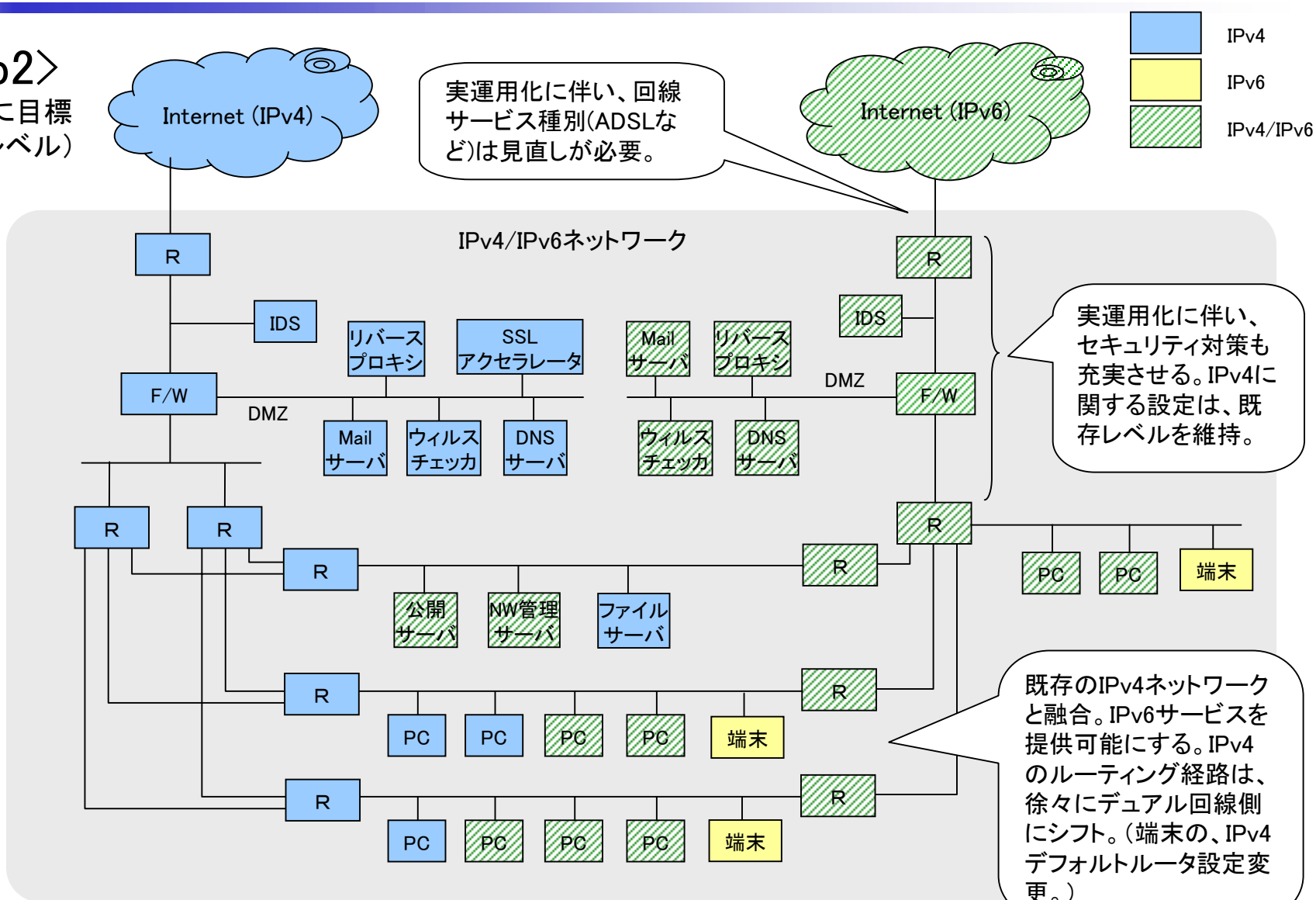


- 既存IPv4ネットワークとは独立に、IPv4/IPv6ネットワークを構築。

- 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。

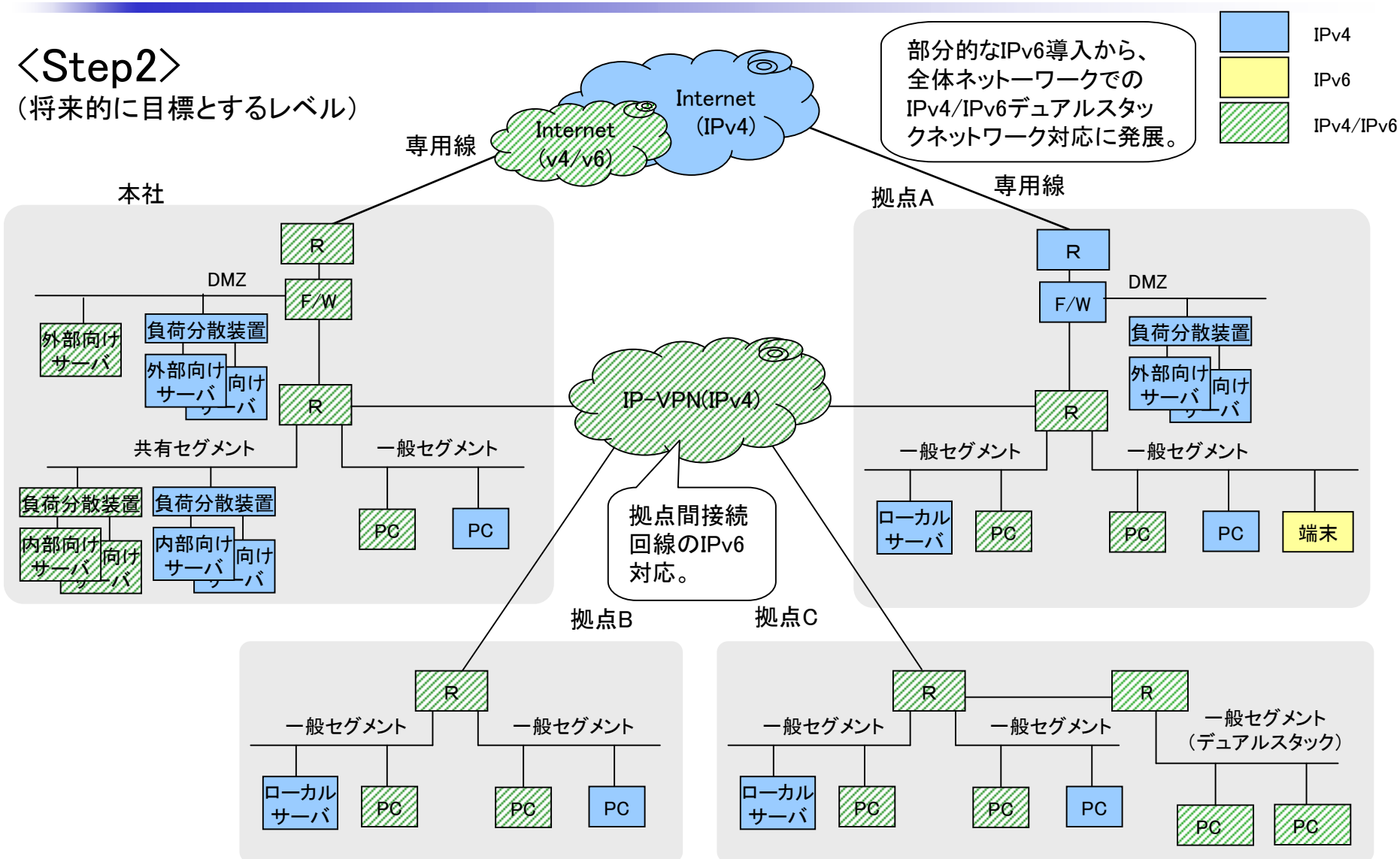
独立融合型： パターンA

〈Step2〉
（将来的に目標とするレベル）



独立融合型： パターンB

〈Step2〉
（将来的に目標とするレベル）



アプリケーション： IPv6で実現したいこと

「Plug & Play + Secure + Managable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 vs 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来る。

セキュリティ
- ・E2E通信は、全ての端末間で許可か？ それとも、特定の端末間のみか?
- ・特に外との間のE2Eの暗号化はOK?
- ・管理者が任意の通信をチェックできるか?

“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 (大体SIP)
- ・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

5:5に向かうための課題

- マルチホーム
- ネットワークアクセス制御
- その他の5:5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＞

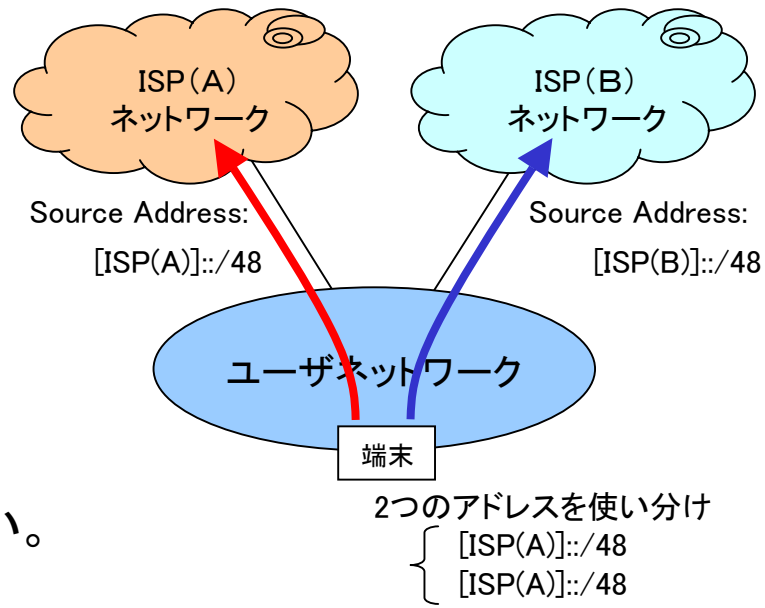
- インターネットへの接続に冗長性が確保される。
- 経路最適化や負荷分散が設定可能。

→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。

ネットワークアクセス制御 （1/2）

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る。

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，，，

全ての機器に自由なアクセスを許可する必要はない！
全ての機器を同一レベルで管理する必要はない！

＜解決策＞

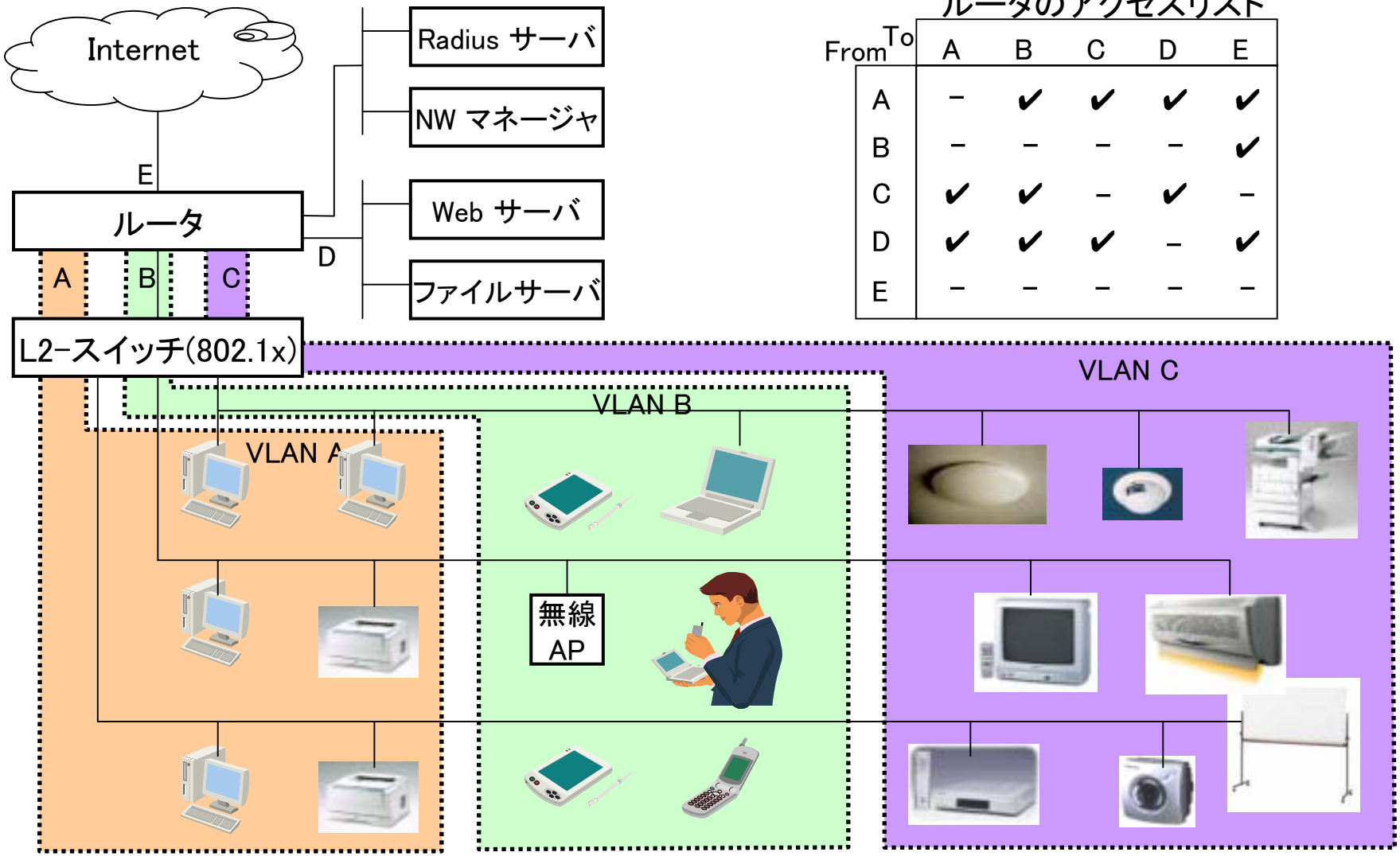
- VLANを使用して幾つかのセグメントに分割。
- IEEE802.1x認証を利用して、機器を適当なセグメントに接続させる。
- セグメント毎にアクセス制限を設ける。

＜アクセスポリシーの例＞

メンバ PC ： 全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。

ネットワークアクセス制御 (2/2)

<IEEE802.1x と VLAN を利用したアクセス制御イメージ>



ルータのアクセスリスト

From \ To	A	B	C	D	E
A	–	✔	✔	✔	✔
B	–	–	–	–	✔
C	✔	✔	–	✔	–
D	✔	✔	✔	–	✔
E	–	–	–	–	–

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）

- 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。
- アドレスリナンバリング　（変更のための工数を最小化したい。）
  - 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NW回線から、新規NW回線へ切替える時。
- 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。

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
- 玄関モデルと金庫モデル
- IPsecのF/W越え
- 将来のF/W構成
- セキュリティモデル追加案

セキュリティに関する基本的な考え方

＜IPv4との違い＞

- IPv6では、IPsecが標準実装されること意外、根本的には同等。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。
  - 不正アクセス防止（F/W、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）
  - その他
- 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い。

＜現時点での基本方針＞

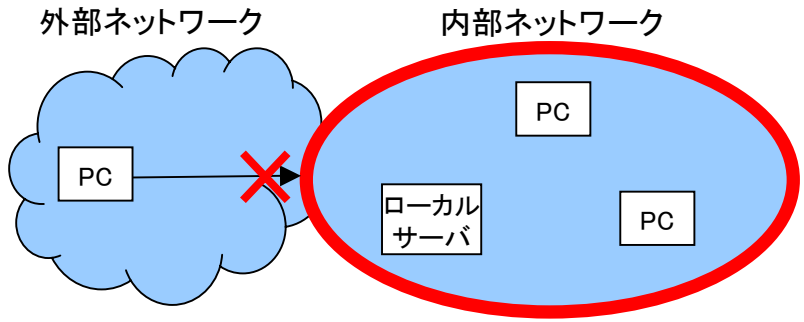
- IPv6におけるセキュリティモデル、及びそれに対応した製品・ソリューションは、まだ完全には確立していない。暫定的なセキュリティポリシを前提としながら、徐々に実用化していく必要がある。

玄関モデルと金庫モデル

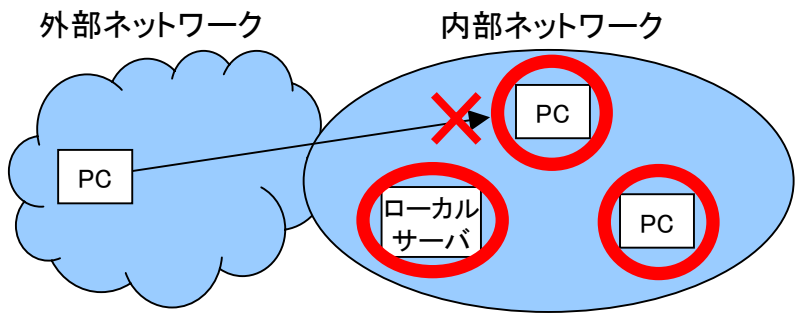
“便利”と“セキュリティ”の共存はなかなか難しい。

- 玄関モデル
  - なんとなく安心。
  - なんとなく管理している感じ。
  - 内部犯罪は想定外。
- 金庫モデル
  - なんとなく不安。
  - 現状、完全性の保障は困難。
  - 柔軟性がある。（リモートアクセス）

→当面はハイブリッドモデルで対応。
将来的には金庫モデルが本命。



玄関モデル

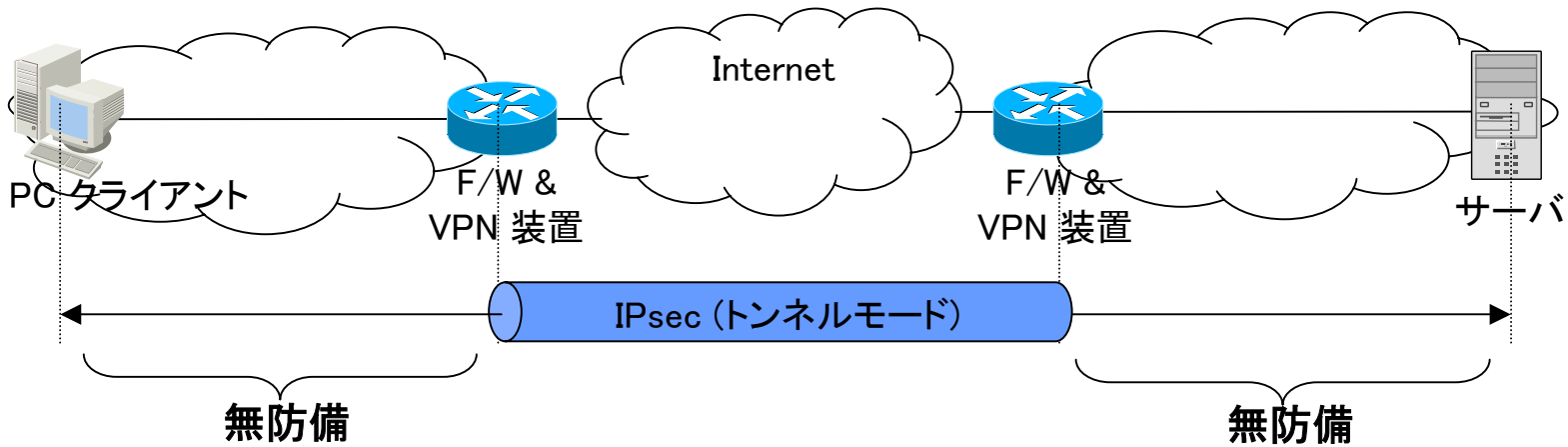


金庫モデル

IPsecのF/W越え(1/4)

＜IPv4セキュリティモデル＞

- VPN装置によるセグメント間のセキュリティ通信



＜問題点＞

- VPN装置と端末間は無防備。
- VPN装置への負荷集中。

- SSLによるセキュリティ通信

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。
特定のアプリケーション(HTTPS)のみ適用可能。

IPsecのF/W越え（2/4）

＜IPv6セキュリティモデル＞

- IPsec を前提としたP2Pセキュリティ通信

  IPsec レイヤ3における暗号化プロトコル。

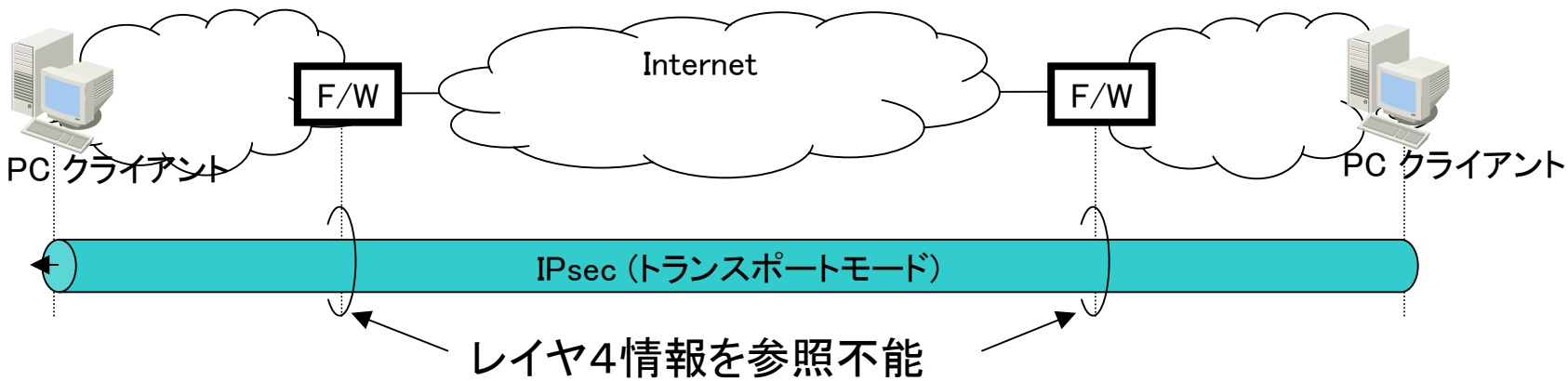
  →アプリケーションに依存することなく適用可能。

  （レイヤ4以上の情報を参照することは出来ない。）

一方、F/Wは レイヤ3，4情報を元にフィルタリングする。

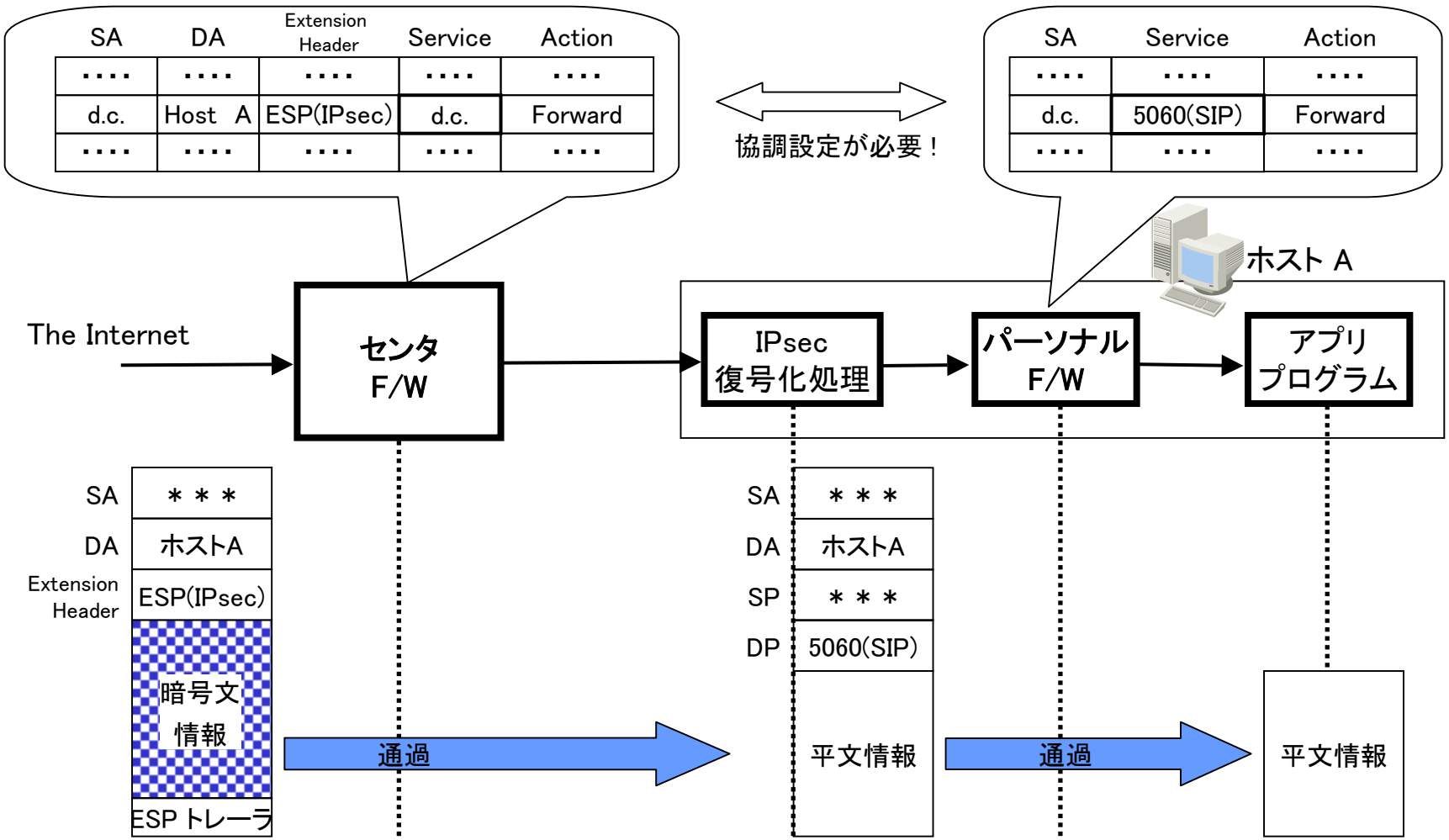
IPsecと(従来の)F/Wを共存させることは不可能。

→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る。



IPsecのF/W越え(3/4)

＜解決策の例＞　:パーソナルF/WとセンタF/Wとの協調フィルタリング



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。

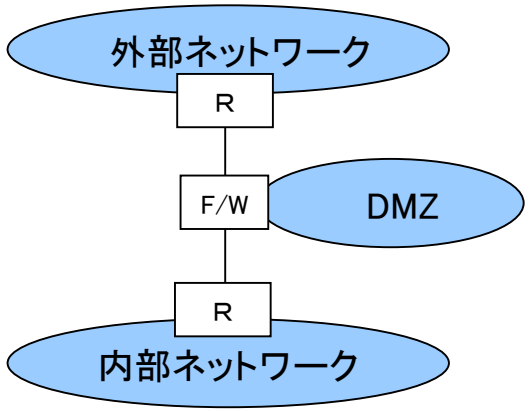
将来のF/W構成

＜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。

＜問題点＞

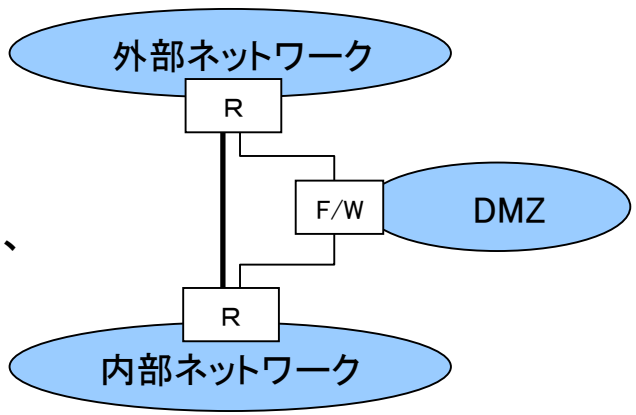
- ブロードバンド化に伴い、帯域的にF/Wがボトルネックになりつつある。
- アプリケーションの多様化。（P2Pアプリ、IPsec）



従来のF/W構成

＜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

セキュリティモデル追加案

＜BCPにおけるセキュリティ実施項目＞

- 大企業・自治体ネットワーク特有の要求仕様
  - ロギングできること： 標準(ISO9000, ISMS)対応。
  - 管理者は中身が覗けること、集中管理できること。(どこまでManageするか?)
- 将来E2E通信が実現できるように
  - 内部ネットワークのルーティング情報を公開する。(もちろんフィルタで止める。)
  - アプリケーションゲートウェイは従来通り稼働させる。
  - IPsecの設定容易化、ユーザ/端末認証で利用できるCA環境。
- 内部ネットワークを保護するために
  - エンドホストのセキュリティ維持。(IPv6対応ウィルスチェッカ、パーソナルF/W)
  - F/W、IDS、IPsec製品の調査。
  - 外部からのIPv6によるアクセスを監視、分析する枠組みの確立。

＜5:5におけるセキュリティへの要件＞

- イントラネットーインターネット 境界部分
  - 半自動でE2E通信を許可するシステムが欲しい。
  - マルチホームの時にこのシステムがどう動くかも検討が必要。(標準化が必要)
  - F/W、IDS、IPsec製品の本格的な整備が必要。
- イントラネット内部制限
  - 金庫と玄関の中間： 関所モデルを構築する?
  - ローカルCAが欲しい?

6

Tips

- DNSサーバの設定
- その他

DNSサーバの設定（1/2）

- **正引きの設定**

IPv4
・Aレコード
www IN A 1.2.3.4
IPv6
・AAAAレコード
www IN AAAA 2001:db8::80
・A6レコードは使わないほうが良い。

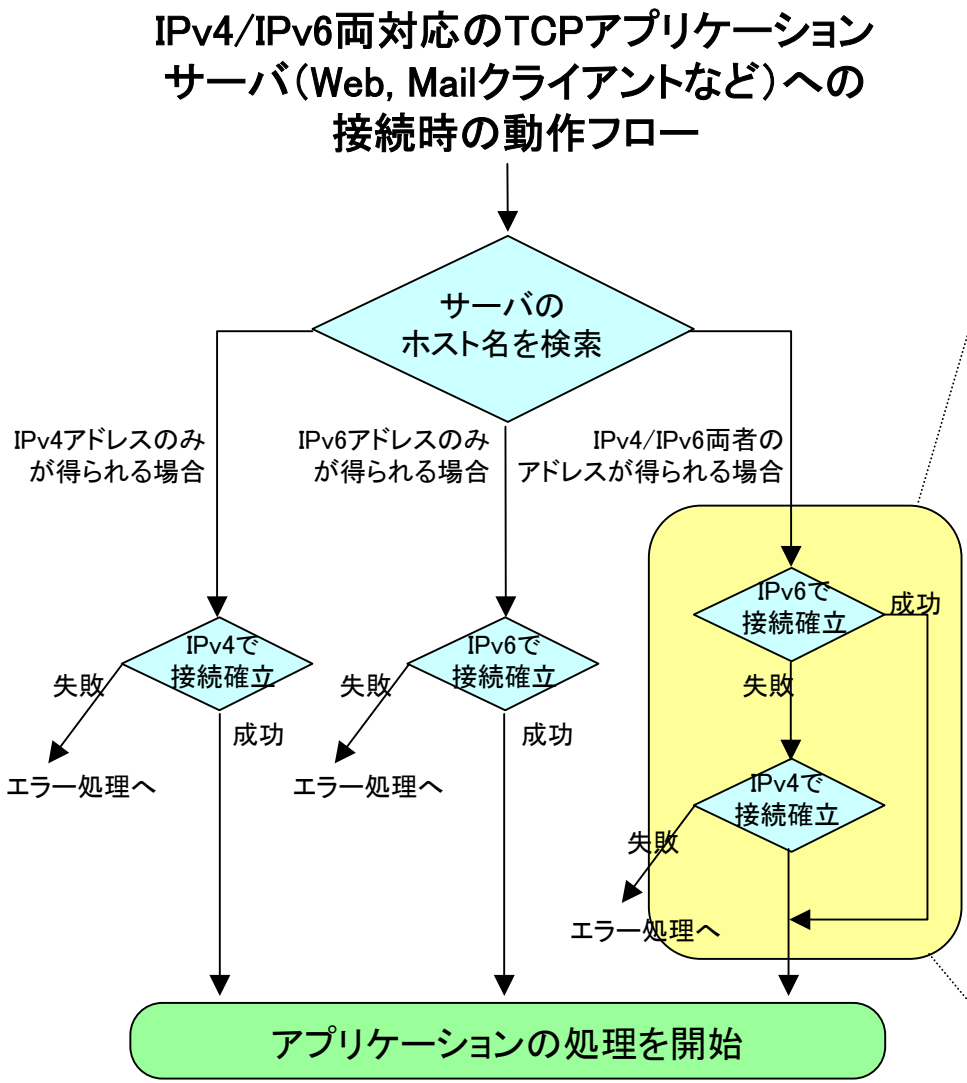
- **逆引きの設定**

IPv4
・ in-addr.arpaドメイン
4.3.2.1.in-addr.arpa IN PTR www.hogehoge.jp
IPv6
・ip6.arpaドメイン
・ip6.intは過去の互換性のため、設定しておくと良い。
0.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6
.arpa IN PTR www.hogehoge.jp

＜IPv6アドレス登録の考え方＞

IPv4アドレスがDNS登録されている既存サービスについて、追加でIPv6対応する際は、
(1)Aレコードと同一のドメイン名を、AAAAレコードでも登録する。
(2)Aレコードとは別のドメイン名を、AAAAレコードで登録する。
の2通りが考えられる。通常、IPv4からIPv6へ移行する場合は、IPv4とIPv6でユーザがドメイン名を使い分ける必要が無い(1)にした方が良いが、意図的にIPv4サービスも継続する場合は、(2)の選択も考えられる。

DNSサーバの設定（2/2）



＜前提＞
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る。

＜問題点＞
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。
失敗と判断されるまで時間を要する為、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る。

＜対策＞
・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。
・「接続不能」を返す仕組み。

MTU Discoveryについて

- IPv4パケットのFragment
  - 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の利用はない
    ⇒ ISPなど、ICMPパケットをフィルタリングするケースもある
- IPv6パケットのFragment
  - IPv6ではパケット配送における経路途中ではFragmentが実施されない。
  - 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送信する。
    ⇒ 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
    ⇒ 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る

その他

- Privacy ExtensionをOFFの方法
- (トンネル、トランスレーション時の)フラグメンテーション関連