HITACHI
Inspire the Next

企業におけるIPv6ネットワーク利用

～IPv6移行の考え方～

(株)日立製作所
ネットワークソリューション事業部
月岡　陽一
y-tsukioka@itg.hitachi.co.jp

目次

HITACHI
Inspire the Next

1. はじめに
   - インターネットの現状とIPv6の位置付け
2. 企業ネットワークの特徴
   - 検討対象とする企業ネットワークの定義付け
3. IPv6移行のためのノウハウ
   - IPv6移行の基本的考え方
   - 各種IPv6移行ノウハウ
   - 暫定的なセキュリティポリシーについて
4. 具体的なIPv6移行イメージ
   - （段階置換型　or　独立・融合型）　×　（パターンA　or　パターンB）
5. 今後の課題
   - IPv6セキュリティモデル
     - 玄関モデルと金庫モデル
     - IPsecのF/W超え
     - 将来のF/Wネットワーク構成
   - マルチホーム
   - 企業内ネットワークアクセス制御
6. まとめ

HITACHI
Inspire the Next

1

はじめに

- インターネットの現状とIPv6の位置付け

インターネットが果たした役割

HITACHI
Inspire the Next

“インターネットは、人類の情報交換手段に革命を起こした”

- 距離概念の形骸化
  世界中の(に)情報を入手(発信)可能
- リアルタイム
  最新の情報を入手(発信)可能
- 低コスト
  あらゆる既存サービスを、低コストで享受(提供)可能
  (商取引、広告、電話、手紙、、、)

既存インターネットの限界

HITACHI
Inspire the Next

- サービス規模・利用分野の拡大
  - 1995年頃から、爆発的に需要が拡大。
  - 回線帯域、サーバ容量、アドレス空間の確保が急務。
- 接続手続き・操作性
  - 子供から老人までが簡単に利用できるGUI。
  - 社会インフラ基盤としての役割。
- セキュリティ・信頼性
  - インターネットを利用した不正行為の増大。
  - ユーザ側のセキュリティに対する“あまい”意識レベル。

→ “新しい枠組みのインターネットプロトコルが必要”

IPv6で何が変わるか

HITACHI
Inspire the Next

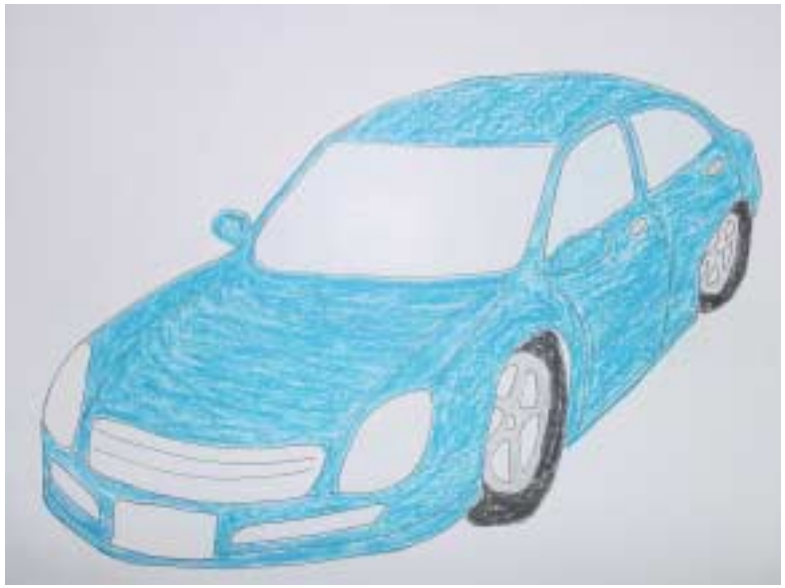
“IPv4で実現できなかったものが、IPv6では実現できるようになる”

と、いうわけではありません。 それでは、IPv6で何が変わるのか？

“IPv4で実現し難かったものが、IPv6では実現し易くなる！”

IPv4とIPv6を自動車に例えるなら、、、

IPv4自動車



IPv6自動車

IPv6： 6つの特徴

HITACHI
Inspire the Next

(1) アドレス空間の拡大

IPv4： 32bitアドレス　$2^{32} = 4.3 \times 10^{9}$
IPv6： 128bitアドレス　$2^{128} = 3.4 \times 10^{38}$

(2) パケットヘッダの簡略化（アドレス体系の階層的管理）

→ルータへの負荷削減、高速化が容易

(3) QoSの強化

Traffic ClassフィールドやFlow Labelフィールドによる、
より効果的なQoS制御

(4) Plug and Play (PnP)

近隣探索プロトコル（NDP)によるIPアドレス自動設定により、
誰もが何処からでも簡単にインターネットを利用可能

(5) セキュリティの強化

End to Endの暗号化、IPsec標準対応

(6) モバイルIP、マルチキャスト

IPv6上で効果的に機能を発揮

IPv6導入のメリット

HITACHI
Inspire the Next

＜企業ネットワークにおけるIPv6のメリット＞

（1） ネットワーク管理のシンプル化
（NAT未使用、Plug＆Play、統一的セキュリティによる。
但し、デュアルスタック環境の管理は、シンプルとは言えない。）

（2） 新規アプリケーションによる業務効率改善
（出張、会議などの効率改善。在宅勤務の可能性）

（3） 組織→個人単位のセキュリティ管理
（確実な認証処理と暗号化通信）

HITACHI
Inspire the Next

2

企業ネットワークの特徴

- 検討対象とする企業ネットワークの定義付け

企業ネットワークの特長

HITACHI
Inspire the Next

- 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

- 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)

企業ネットワークの分類要素（パターンA）

HITACHI
Inspire the Next

(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
- ■ xDSL, CATV, FTTH
- ■ 専用線

(3) ユーザ数（共有サーバへのアクセス量）
- ■ 100人以下（負荷分散不要）
- ■ 100人以上(負荷分散必要)

(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
- ■ 本社集中型
- ■ 部門分散型

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

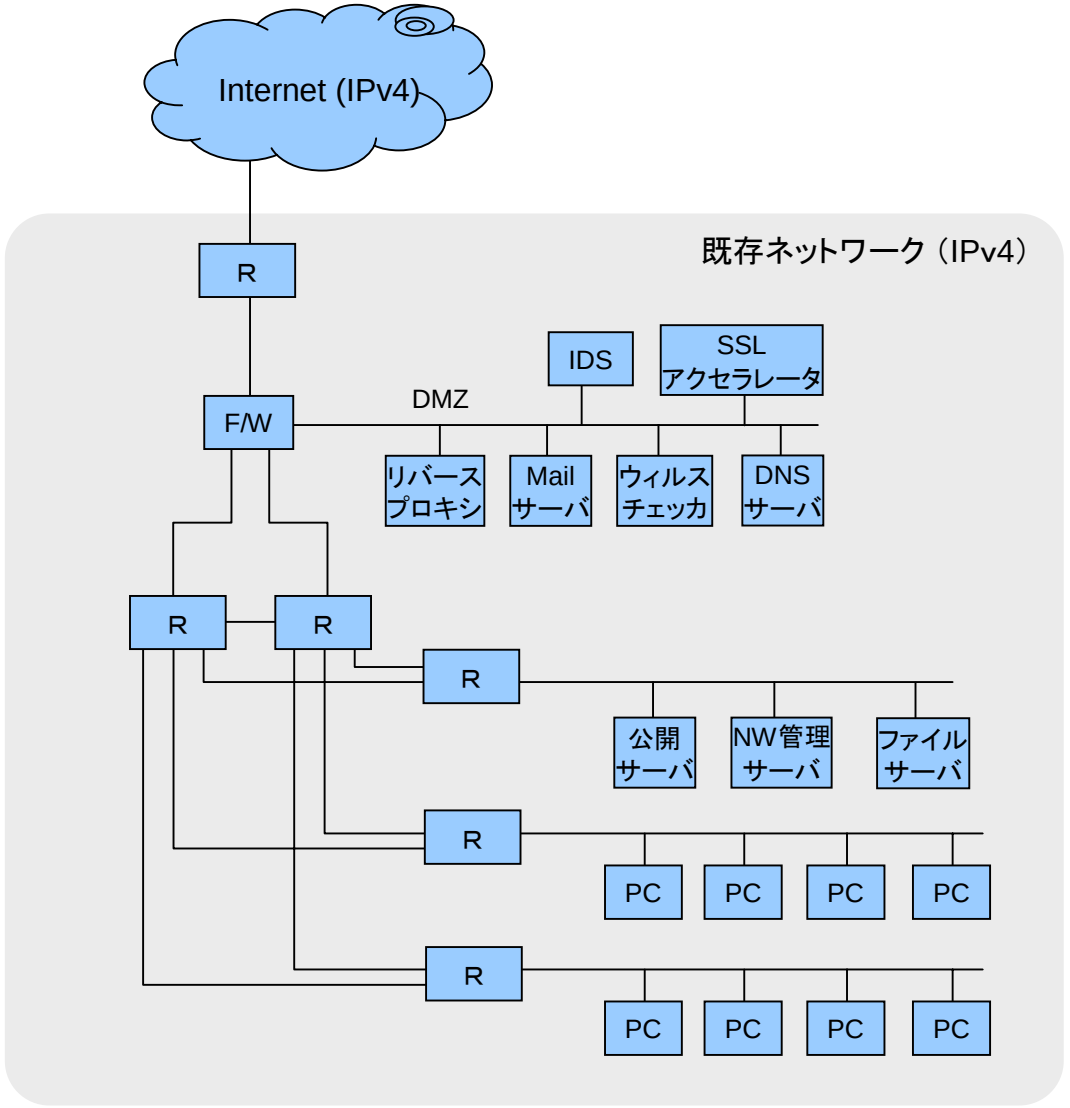
(8) リモートアクセス
- ■ 有り
- ■ 無し

(9) アドレス運用
- ■ グローバル（NAT未使用）
- ■ プライベート（NAT使用）

(10) VoIPの導入
- ■ 有り
- ■ 無し

企業ネットワークの例(パターンA)

HITACHI
Inspire the Next



企業ネットワークの分類要素（パターンB）

HITACHI
Inspire the Next

(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
- xDSL, CATV, FTTH
- ● 専用線

(3) ユーザ数（共有サーバへのアクセス量）
- 100人以下（負荷分散不要）
- ● 100人以上(負荷分散必要)

(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
- ● 本社集中型
- ● 部門分散型

(7) 冗長構成（ISP接続回線、基幹装置など）
- 有り
- ● 無し

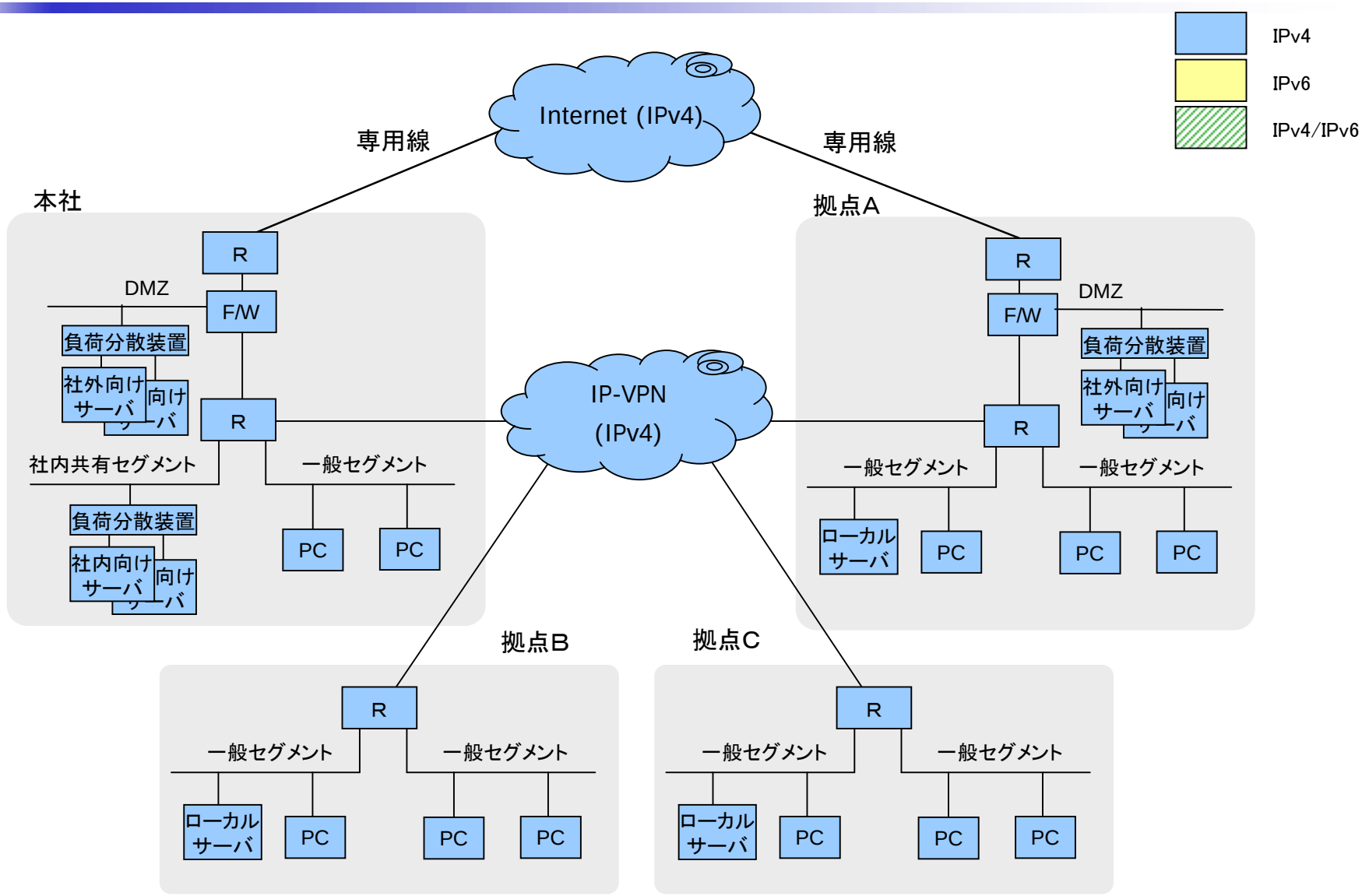
(8) リモートアクセス
- 有り
- ● 無し

(9) アドレス運用
- グローバル（NAT未使用）
- ● プライベート（NAT使用）

(10) VoIPの導入
- 有り
- ● 無し

企業ネットワークの例(パターンB)

HITACHI
Inspire the Next



HITACHI
Inspire the Next

3

IPv6移行のためのノウハウ

- IPv6移行の基本的考え方
- 各種IPv6移行ノウハウ
- 暫定的なセキュリティポリシーについて

基本方針

HITACHI
Inspire the Next

＜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。
- 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。

IPv6対応サービス・機器について(1)

HITACHI
Inspire the Next

“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)

HITACHI
Inspire the Next

＜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。

IPv6対応サービス・機器について(3)

HITACHI
Inspire the Next

今後、IPv6対応が期待されるもの

- ロードバランサ
- セキュリティ関連装置(F/W、IDS、ウィルスチェッカ、)
- 携帯電話
- 家電、自動車、センサ、などのnon-PC系端末
- 各種アプリケーション。。。

IPv6グローバルアドレスの取得と運用

HITACHI
Inspire the Next

＜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。

＜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、殆どの企業ユーザで十分なアドレス空間。
とは言え、将来の展開を考慮し、下記の項目に留意すべき。

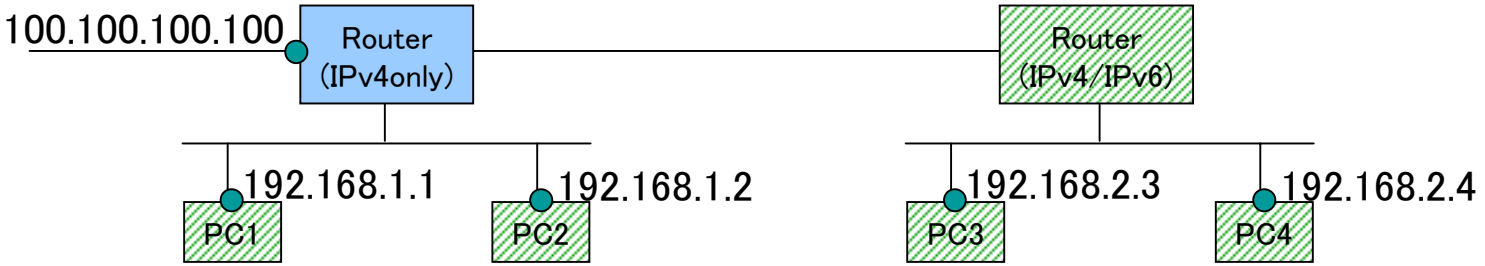
- シンプルで効率の良い（見易い）アドレスの割付け
- 将来予想されるネットワーク構成の組換え・拡大を想定した、階層的なアドレス割付け
- 企業における地理的・組織的な構成に合せたアドレス割付け

IPv6 ローカルアドレス付与方法

HITACHI
Inspire the Next

“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まった。 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) 6to4によるアドレス生成ルールを利用



	IPv4 address	IPv6 address
PC1	192.168.1.1	2002:6464:6464:1:0000:5efe:c0a8:0101
PC2	192.168.1.2	2002:6464:6464:1:0000:5efe:c0a8:0102
PC3	192.168.2.3	2002:6464:6464:2: [EUI-64]
PC4	192.168.2.4	2002:6464:6464:2: [EUI-64]

ISATAP 192.168.1.2

6to4 100.100.100.100

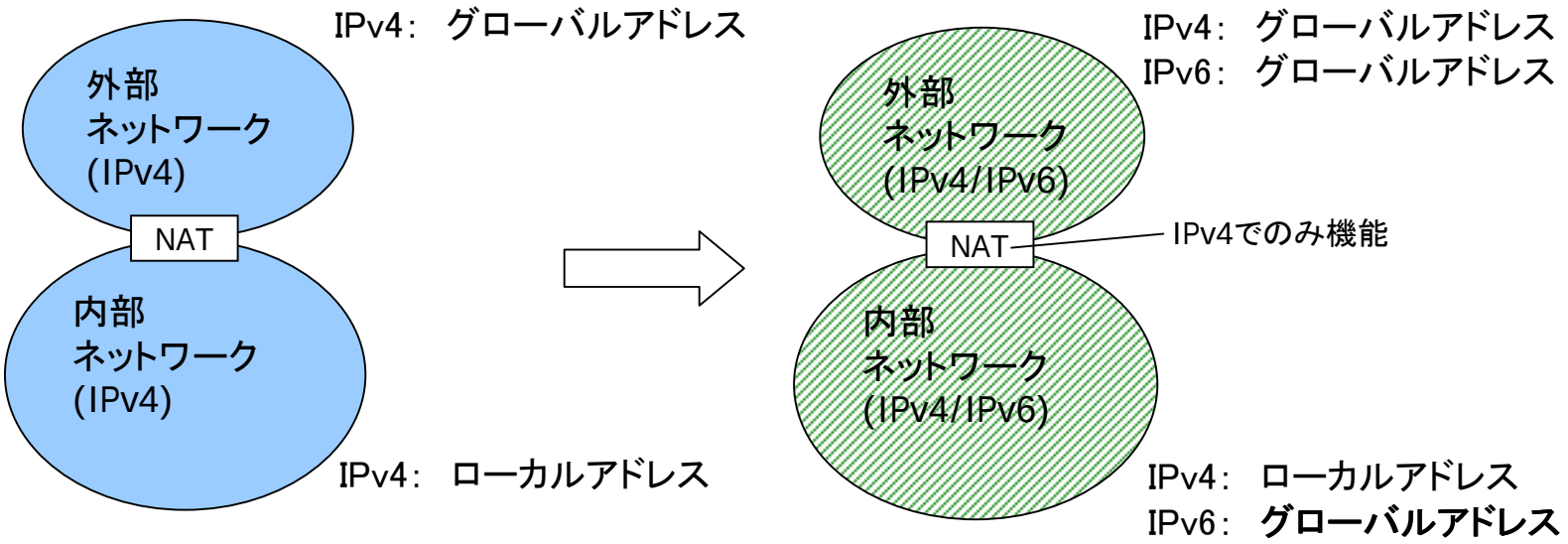
(2) グローバルユニーク・ローカルアドレス (fc00::/8, fd00::/8)

→ 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。

NAT

HITACHI
Inspire the Next

- 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すべきではない。(使用する必要が無い。)**



※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)する例もある。

ルーティング

HITACHI
Inspire the Next

＜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。

＜企業ネットワークにおける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。
- 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。

トンネリング

HITACHI
Inspire the Next

＜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＞

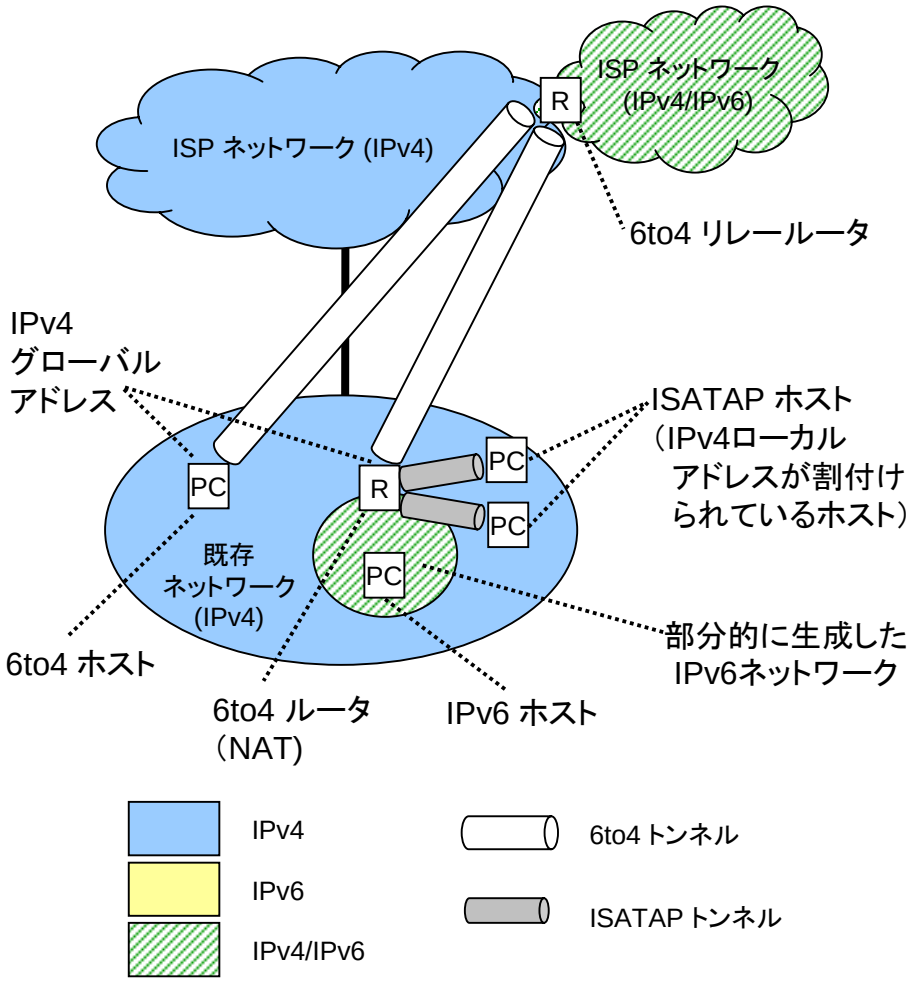
- DTCP（Dynamic Tunneling Control Protocol）
  - クライアント側から動的にトンネル生成を要求可能
    （例： フリービット： Feel6 Farm IPv6接続実験）
- 6to4
  - グローバルIPv4アドレスからIPv6アドレスを自動生成(※1)
  - 主要ISPなどが供給する6to4リレールータとの間でトンネルを生成
  - 往路と復路の経路が同一になる保障が無い
- ISATAP
  - ローカルIPv4アドレスが運用されているLANの中でトンネルを生成可能
- Teredo
  - NATデバイスが介在する環境においてトンネル技術を利用可能

(※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。

自動トンネリング

HITACHI
Inspire the Next

自動トンネリングプロトコル(6to4,ISATAPなど)を利用して、
暫定的にIPv6を導入。

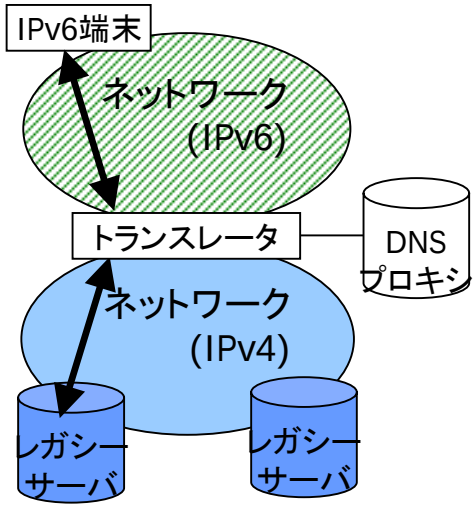


- 公開されている6to4リレールータとIPv4グローバルアドレスを持つルータ／ホスト間で、6to4トンネルを生成。
- 6to4ルータとIPv4グローバルアドレスを持たないホスト間では、ISATAPトンネルを生成。
- トンネル生成区間にF/Wなどが存在する場合、IPv6overIPv4パケット(IPプロトコル番号41のパケット)を通過させる設定が必要。
- 比較的容易にIPv6導入可能だが、パフォーマンス、信頼性、セキュリティなどの問題が有る。
- 6to4トンネルの場合、転送されるパケットの往路と復路が同一になる保障は無い。

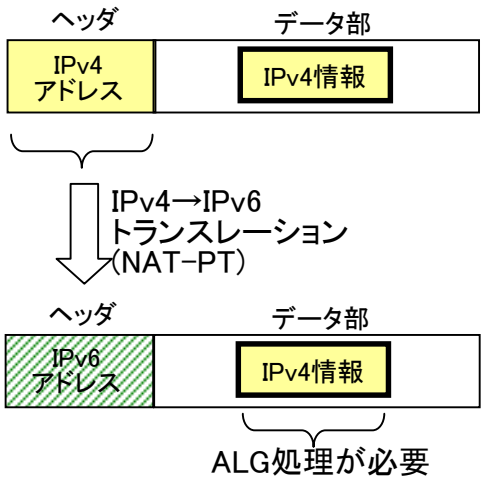
トランスレータ

HITACHI
Inspire the Next

- 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）



- 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



企業ネットワークのセキュリティ

HITACHI
Inspire the Next

企業・自治体組織においては、“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、FWに穴を開ける
- IPv6の特長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

“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！”

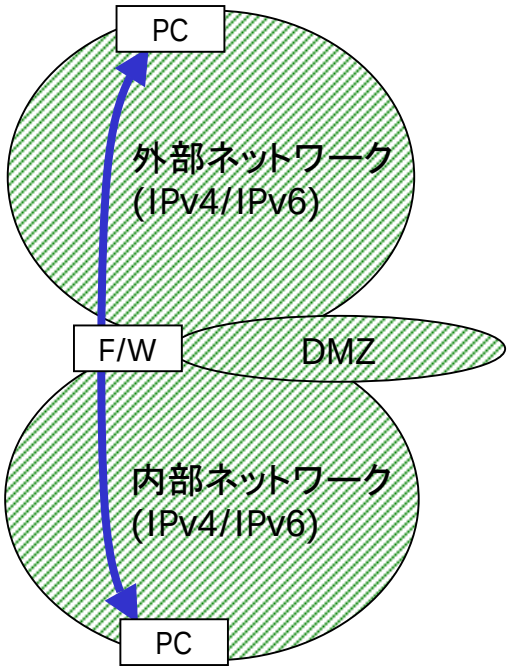
ファイアウォール（1）

HITACHI
Inspire the Next

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。
- IPsec通信のF/Wを経由するE2EIPsec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。）

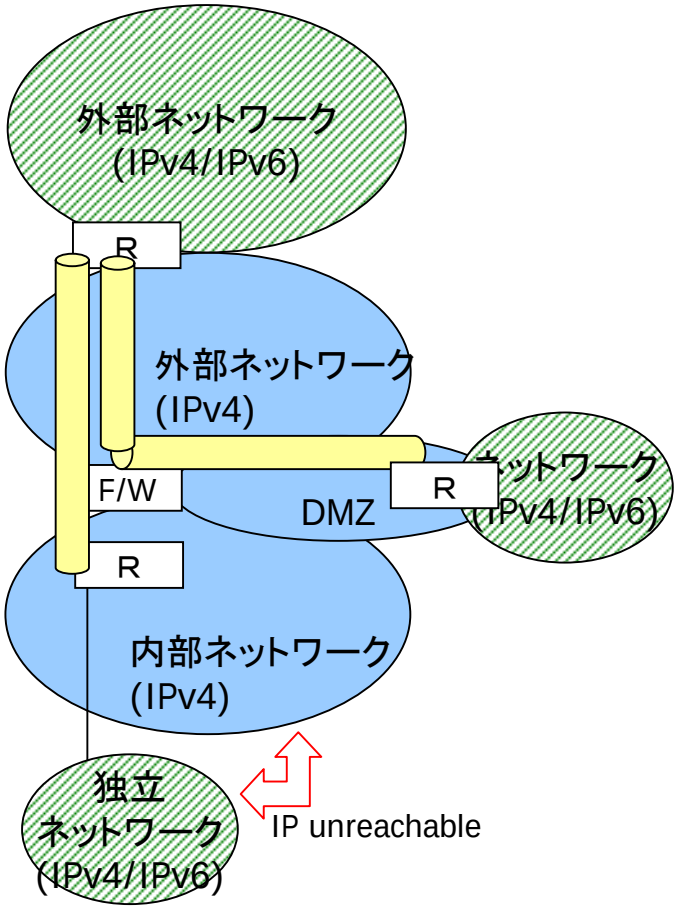


ファイアウォール（2）

HITACHI
Inspire the Next

＜IPv6overIPv4トンネリングについて＞

- IPv6未対応のF/Wなどにおいて、IPv6overIPcv4トンネル通信を許容する場合、基本はDMZにおいて終端する。
- IPv6未対応のF/Wなどにおいて、IPv6overIPv4トンネル通信を内部ネットワークへ許容する（IPプロトコル番号41を通過させる）場合、当面は既存ネットワークとは独立したネットワーク（IPunreachable）で試行すべき。



アプリケーションのIPv6対応の進め方

HITACHI
Inspire the Next

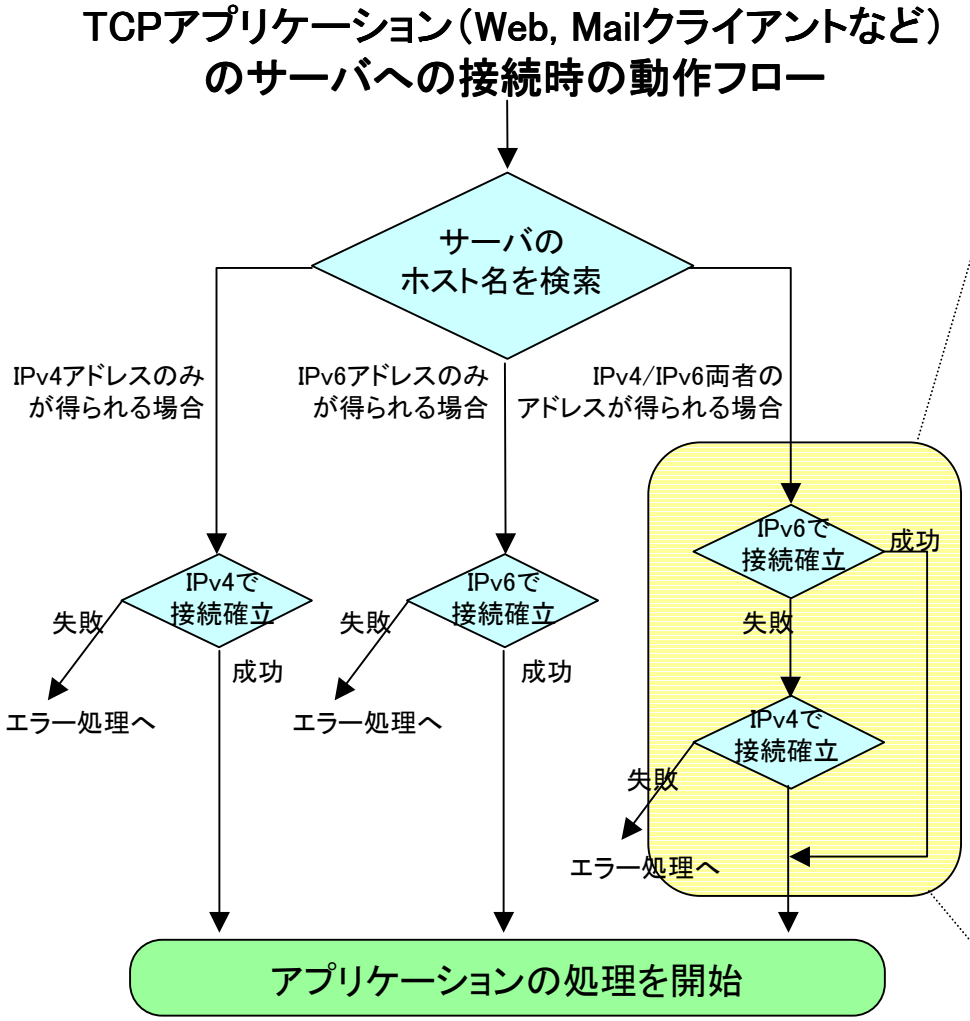
1. 新規アプリケーションはデュアル対応をデフォルトとする。

2. 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。もしくは、
   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対応を進める。）

3. 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。

IPv4/IPv6両対応アプリケーションの問題点

HITACHI
Inspire the Next



＜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

HITACHI
Inspire the Next

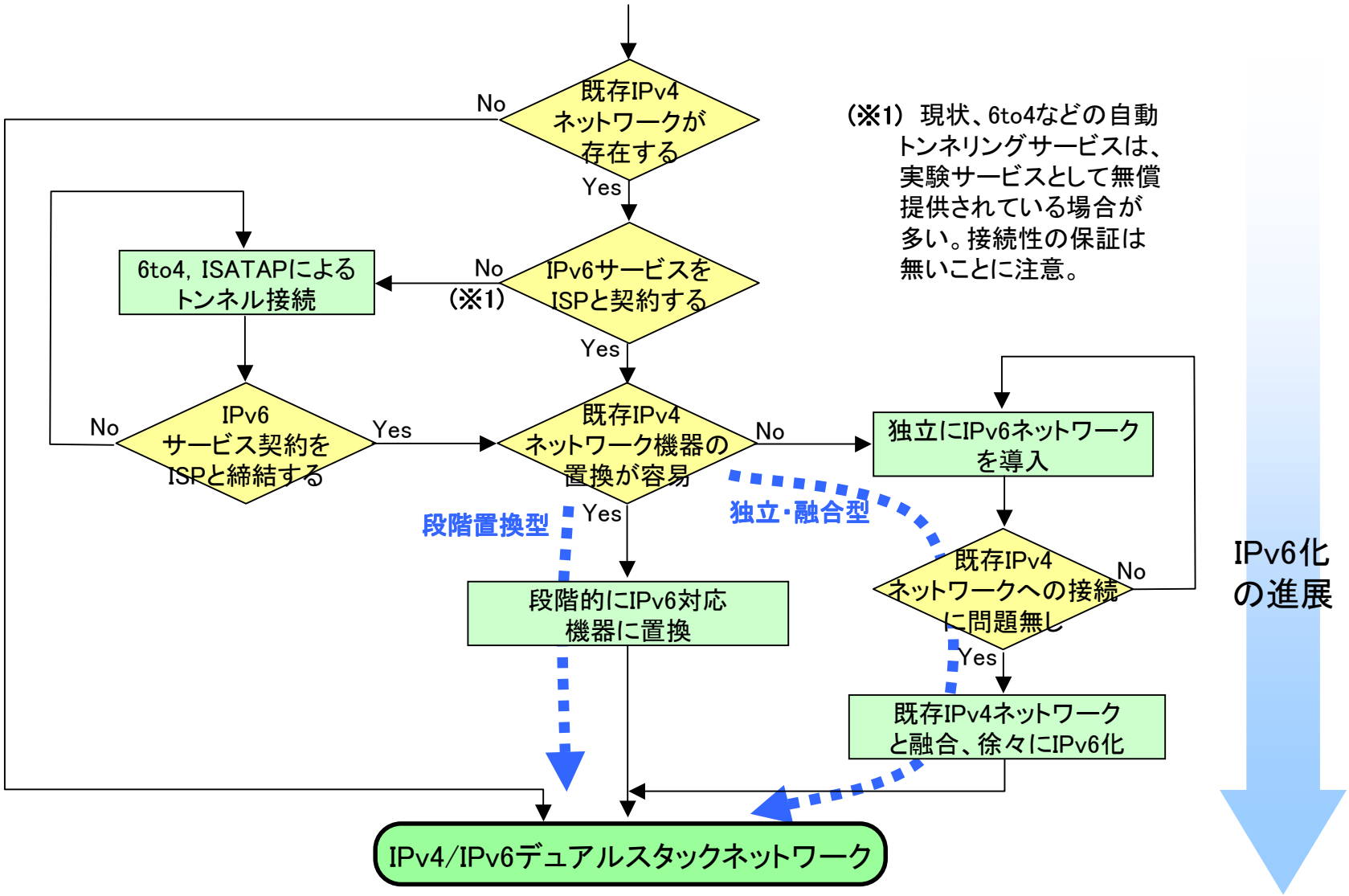
4

具体的なIPv6移行イメージ

- （段階置換型　or　独立・融合型）　×　（パターンA　or　パターンB）

IPv6 ネットワーク構築のフロー

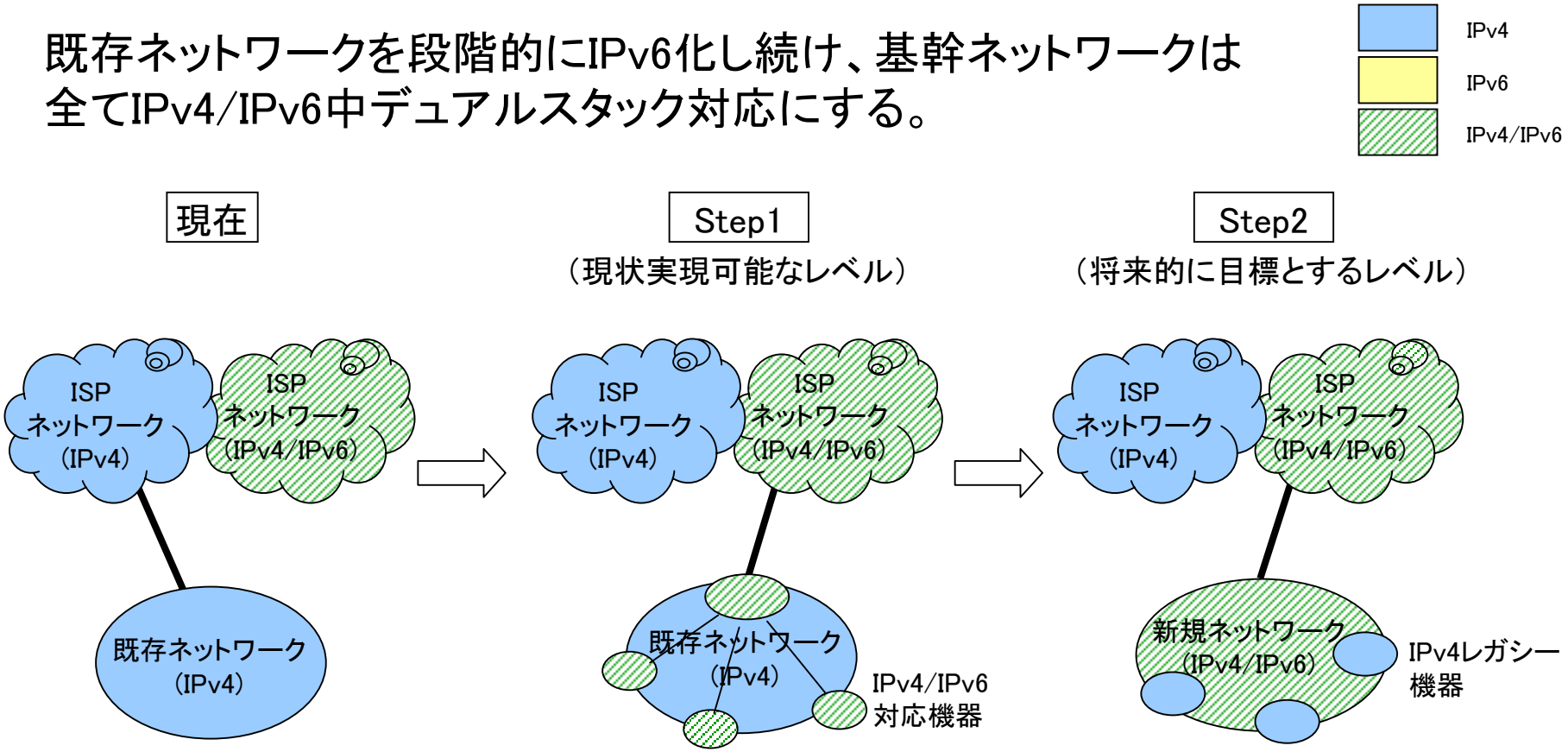
HITACHI
Inspire the Next



段階置換型の移行パターン

HITACHI
Inspire the Next

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。



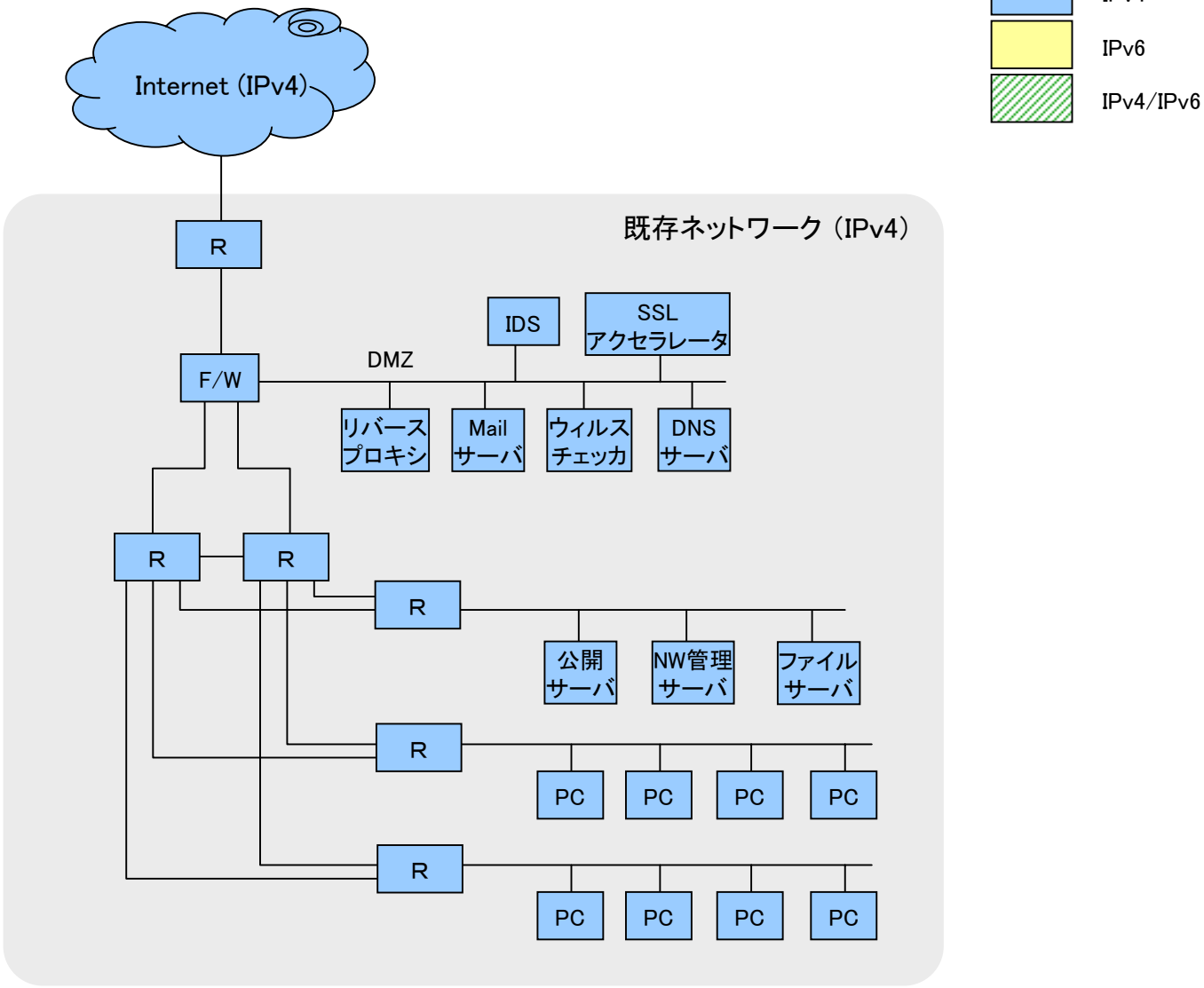
・既存IPv4ネットワークの
一部を段階的にIPv6対応
機器に置換していく

・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

HITACHI
Inspire the Next

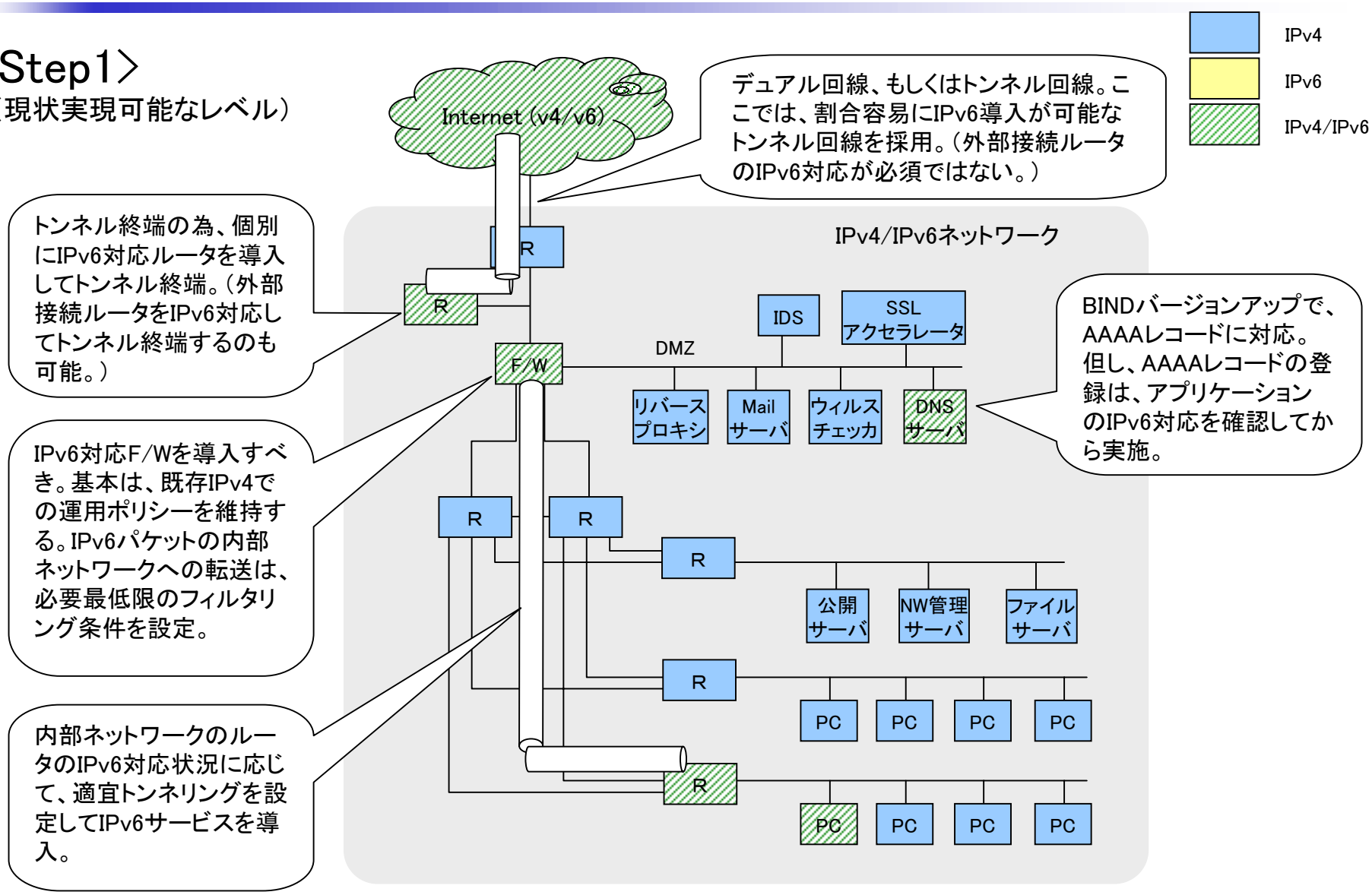
〈移行前〉



段階置換型： パターンA （1）

HITACHI
Inspire the Next

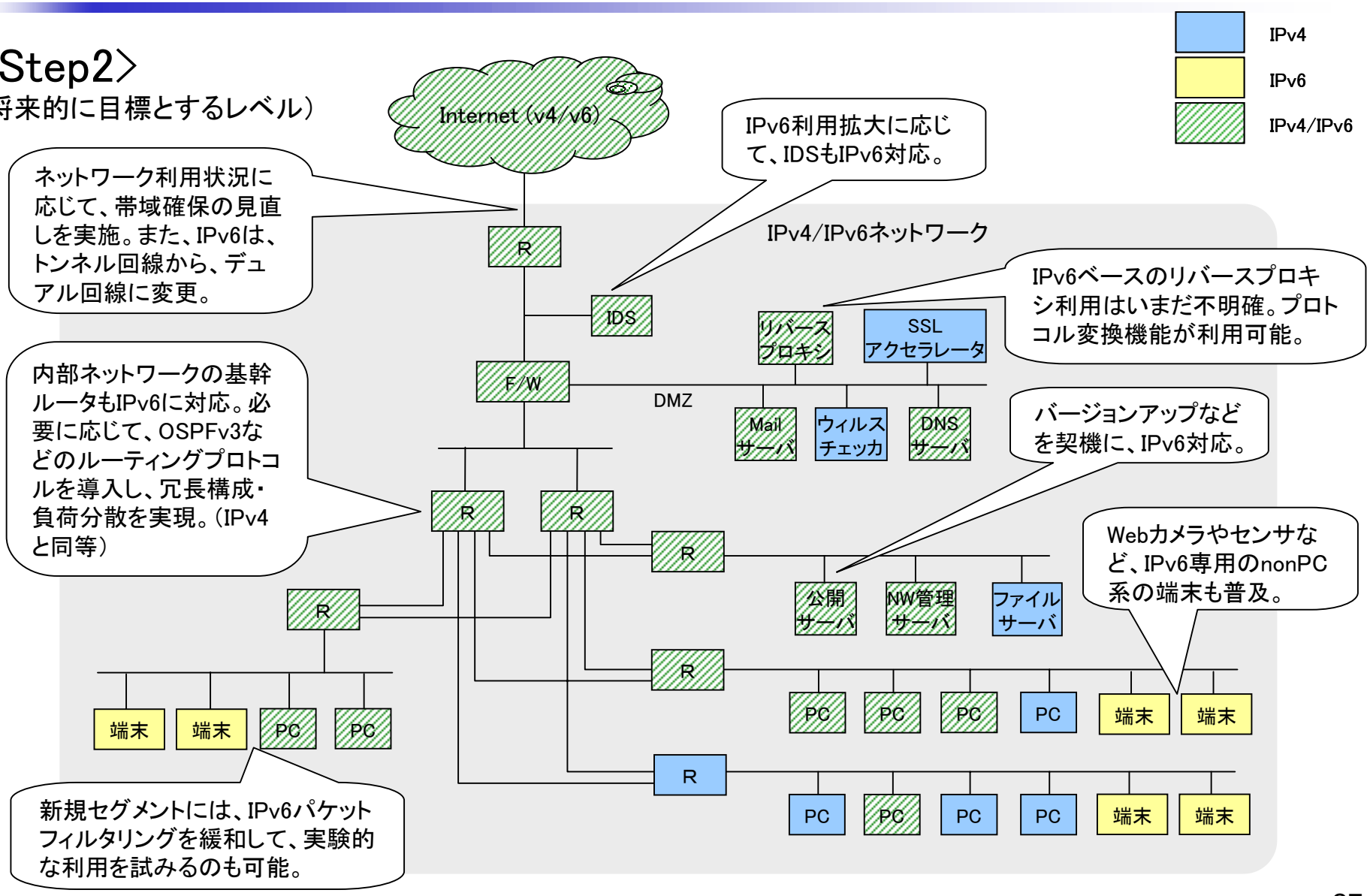
〈Step1〉
（現状実現可能なレベル）



段階置換型： パターンA （2）

HITACHI
Inspire the Next

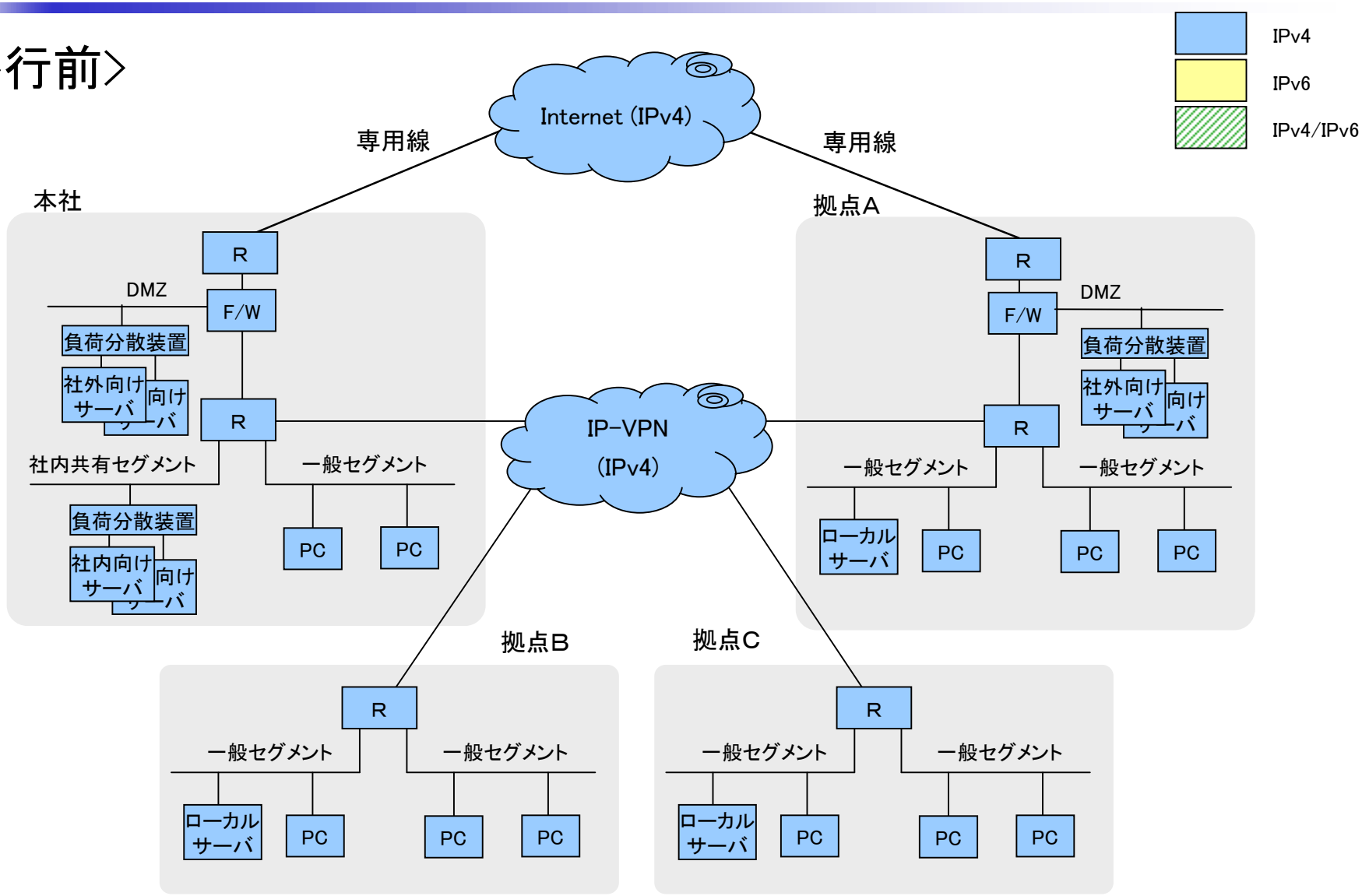
〈Step2〉
（将来的に目標とするレベル）



段階置換型： パターンB

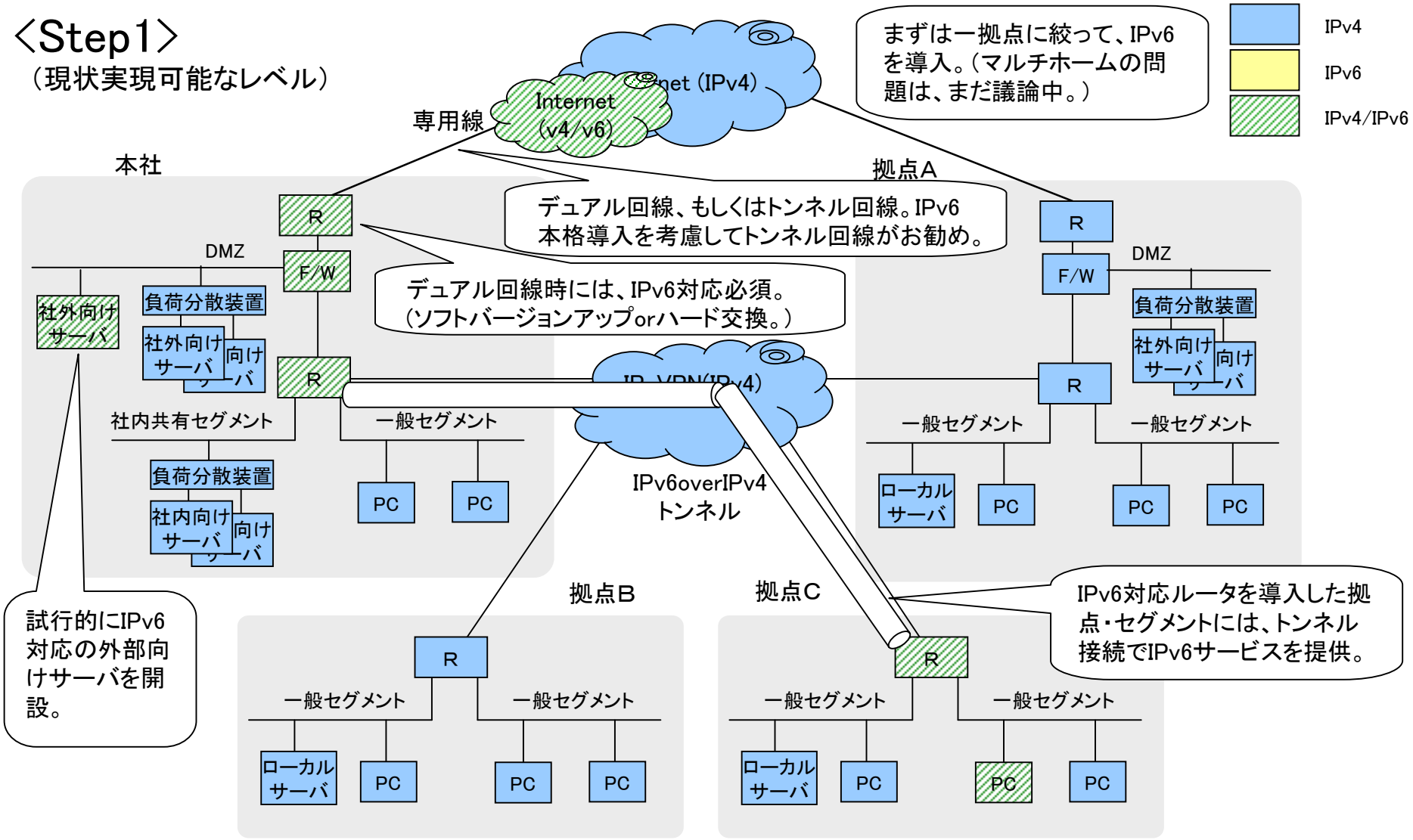
HITACHI
Inspire the Next

〈移行前〉



段階置換型： パターンB （1）

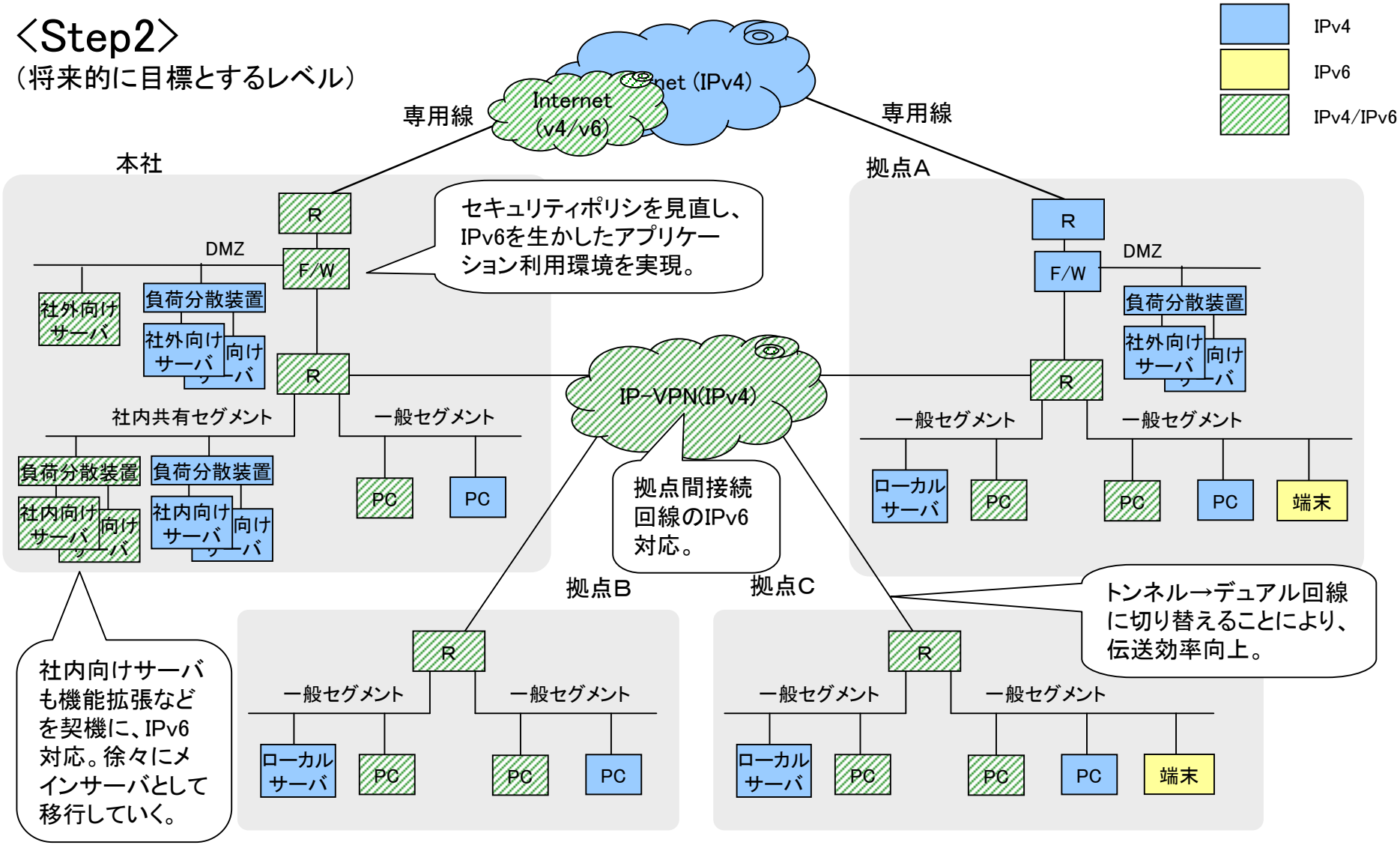
HITACHI
Inspire the Next



段階置換型： パターンB （2）

HITACHI
Inspire the Next

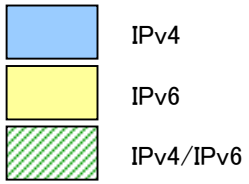
〈Step2〉
（将来的に目標とするレベル）

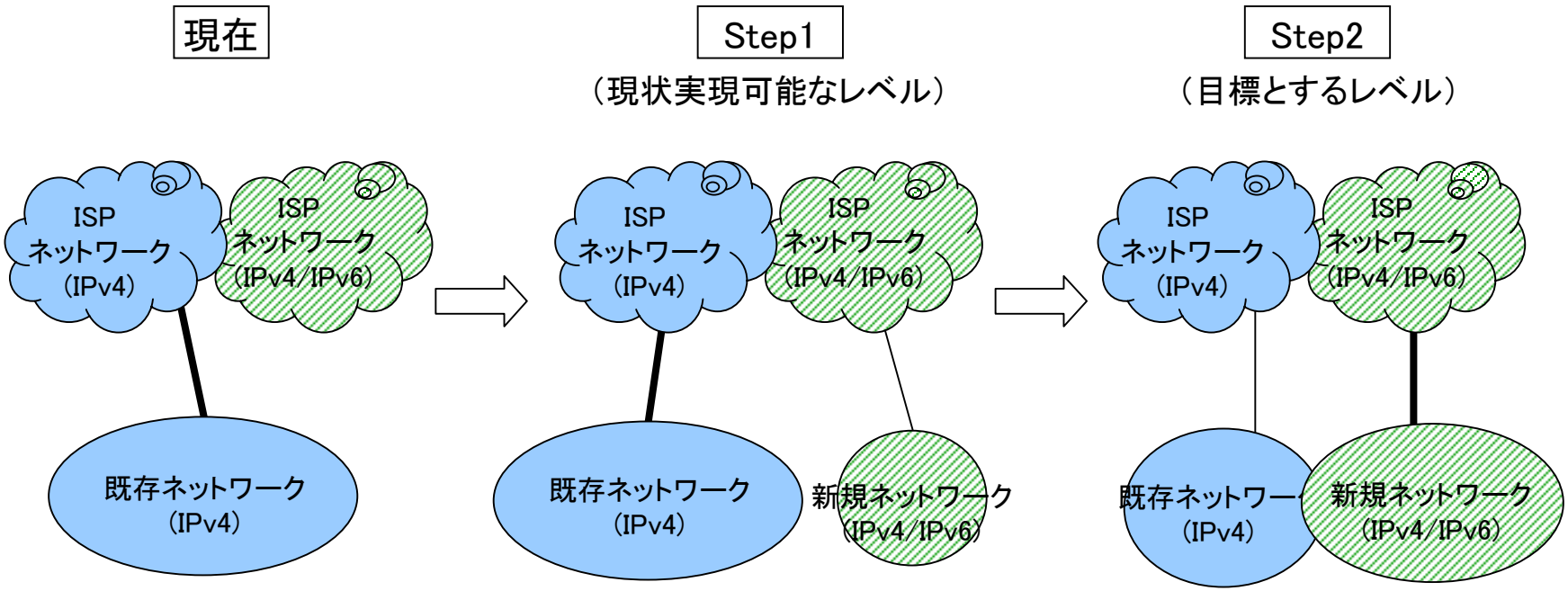


独立・融合型の移行パターン

HITACHI
Inspire the Next

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





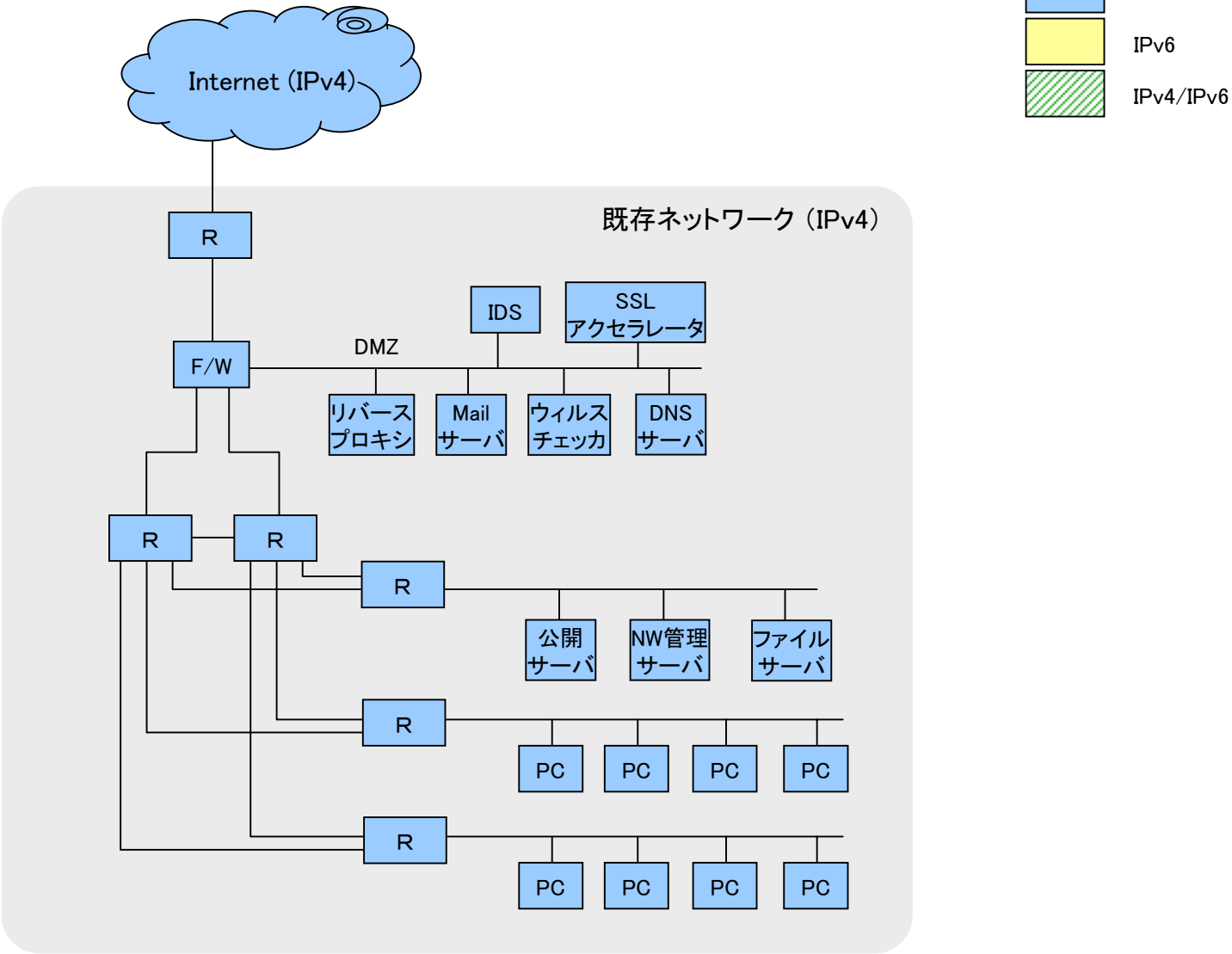
・既存IPv4ネットワークとは独立に、IPv4/IPv6ネットワークを構築

・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

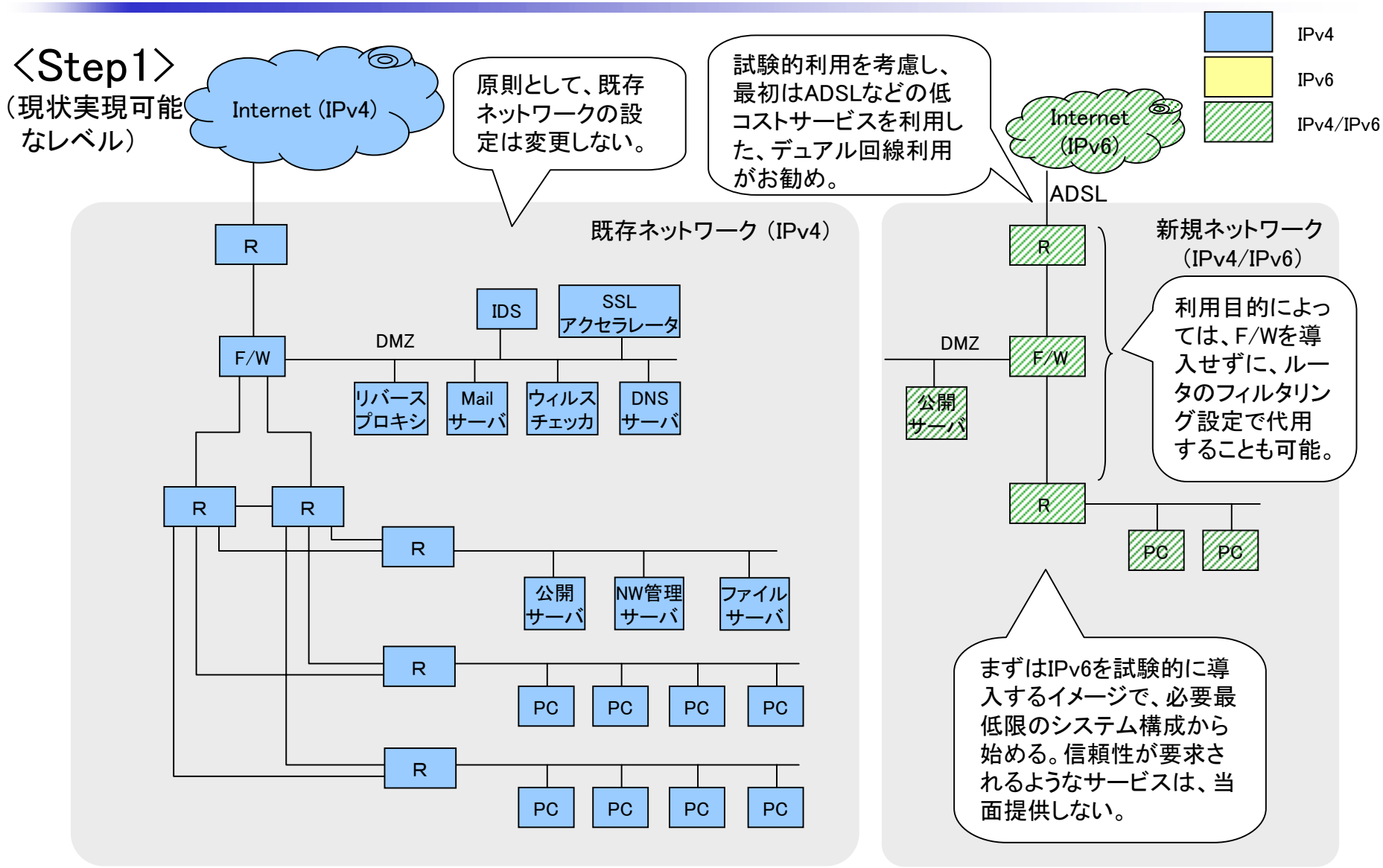
HITACHI
Inspire the Next

〈移行前〉



独立・融合型： パターンA（1）

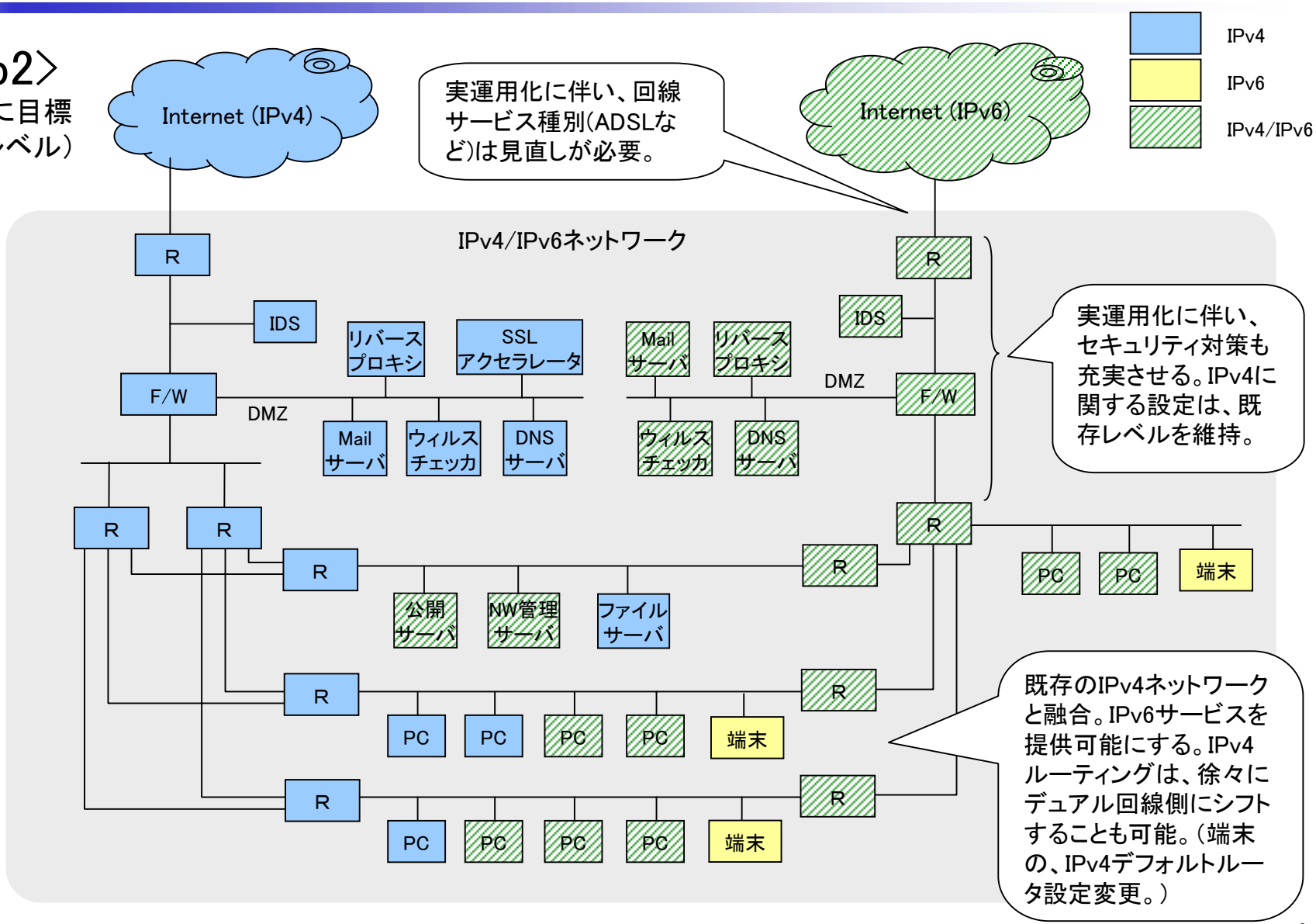
HITACHI
Inspire the Next



独立・融合型： パターンA （2）

HITACHI
Inspire the Next

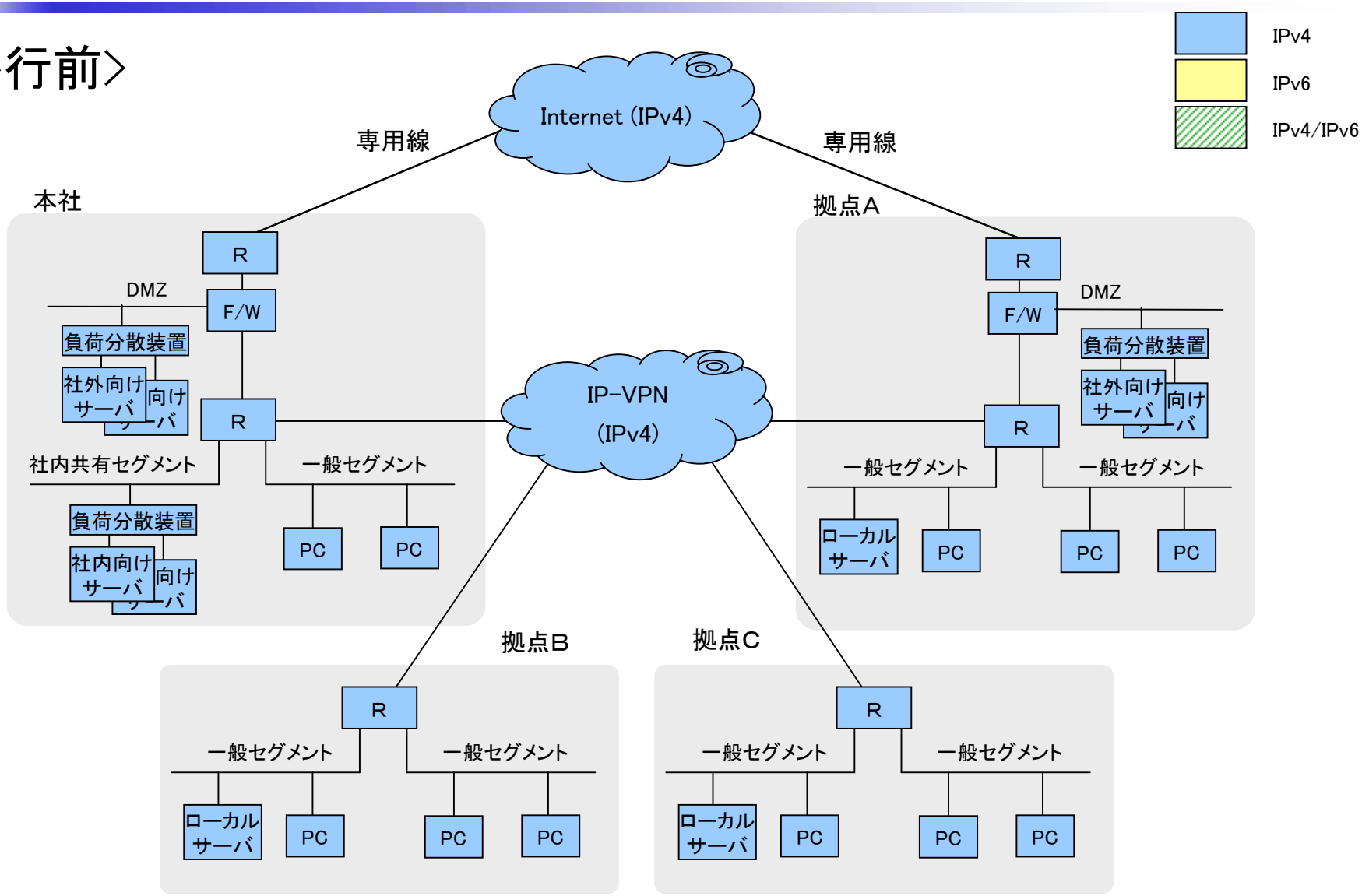
〈Step2〉
（将来的に目標とするレベル）



独立・融合型： パターンB

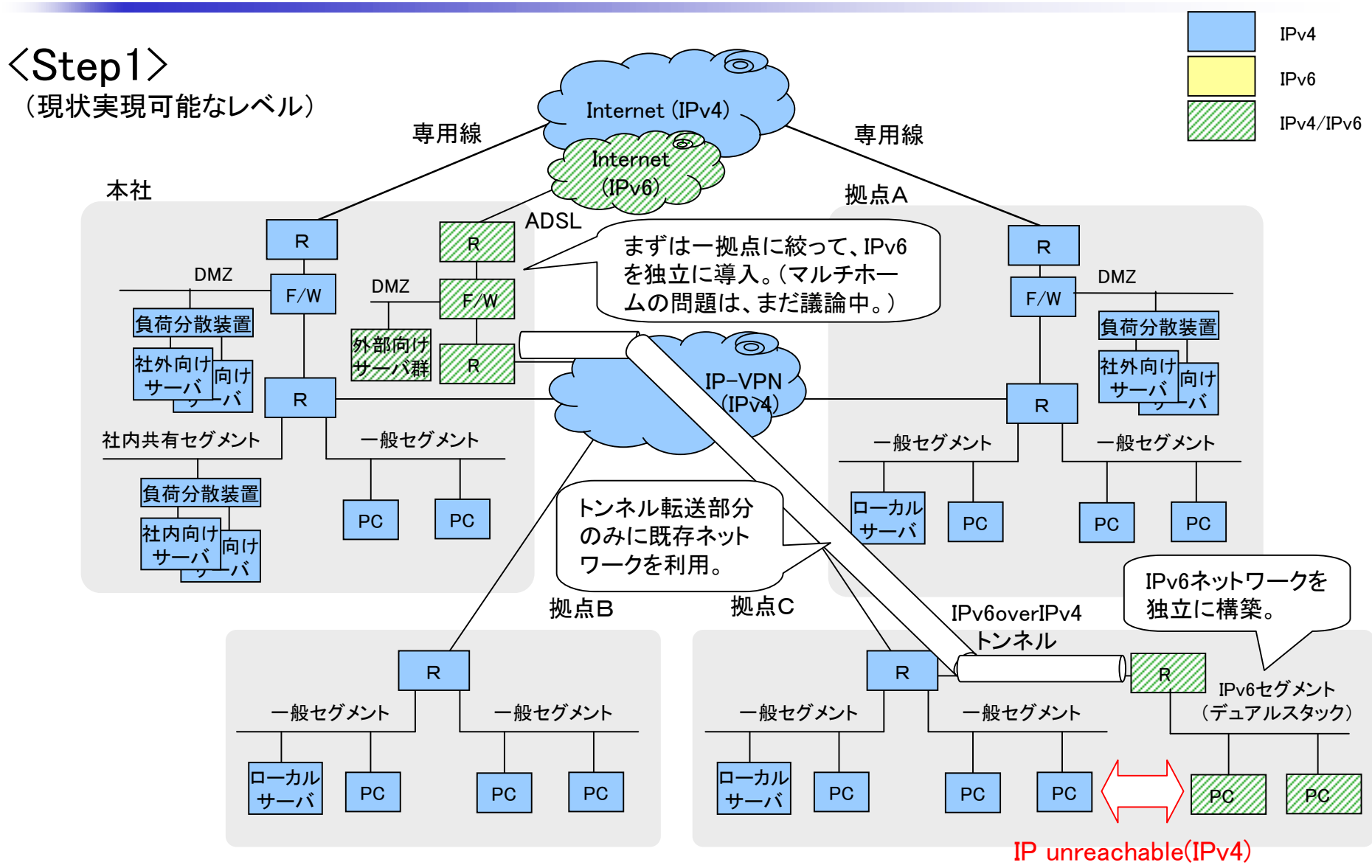
HITACHI
Inspire the Next

〈移行前〉



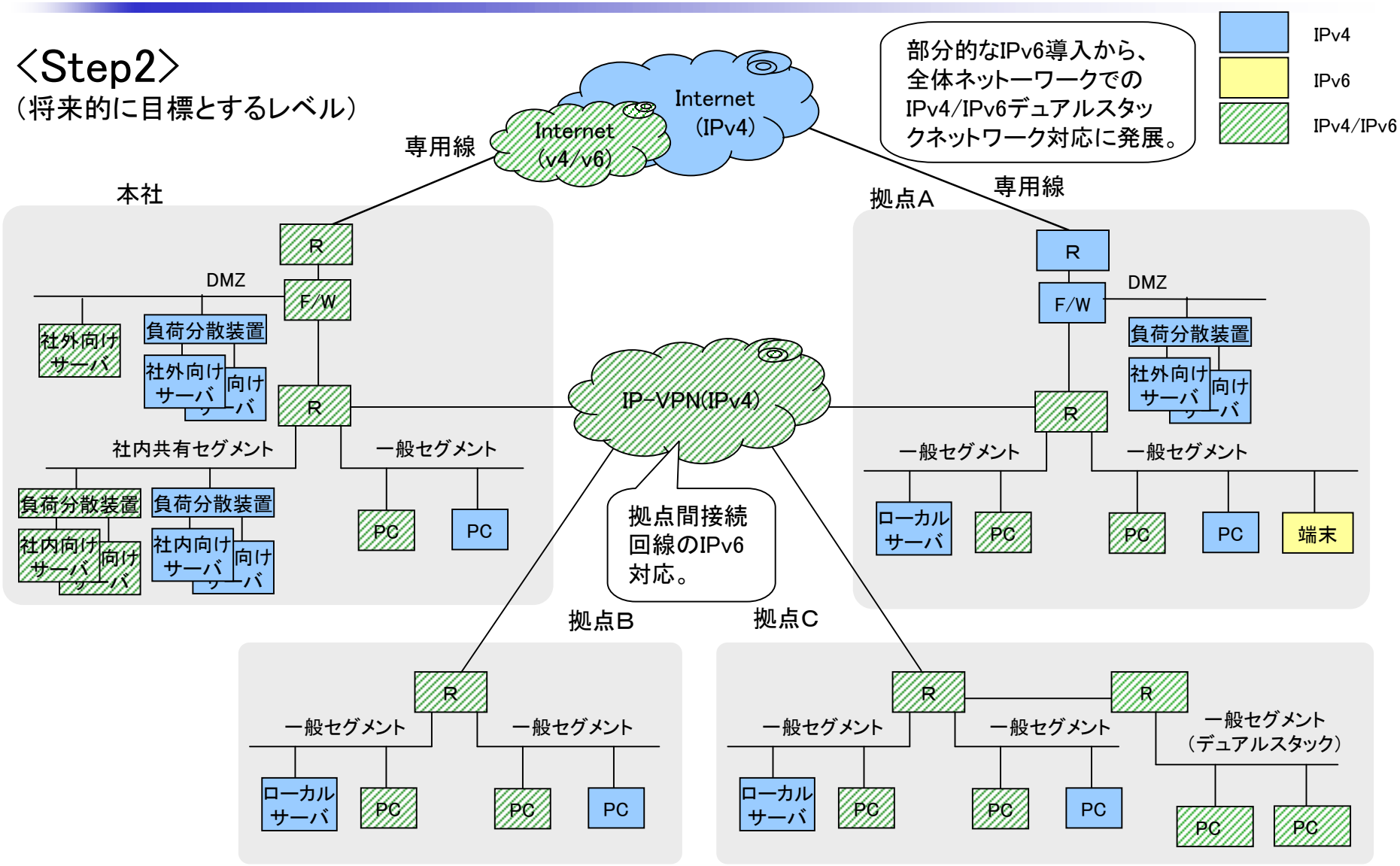
独立・融合型： パターンB （1）

HITACHI
Inspire the Next



独立・融合型： パターンB （2）

HITACHI
Inspire the Next



HITACHI
Inspire the Next

5

今後の課題

- IPv6セキュリティモデル
  - 玄関モデルと金庫モデル
  - IPsecのF/W超え
  - 将来のF/Wネットワーク構成
- マルチホーム
- 企業内ネットワークアクセス制御

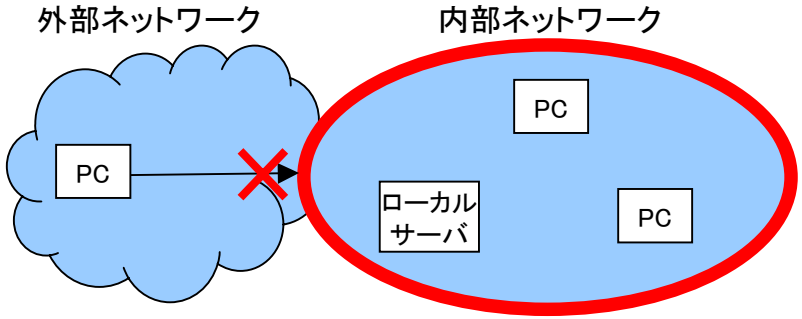
セキュリティモデル

HITACHI
Inspire the Next

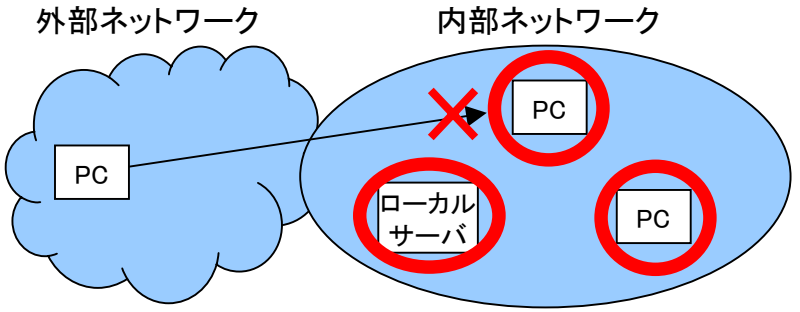
“便利”と“セキュリティ”の共存はなかなか難しい。

- 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



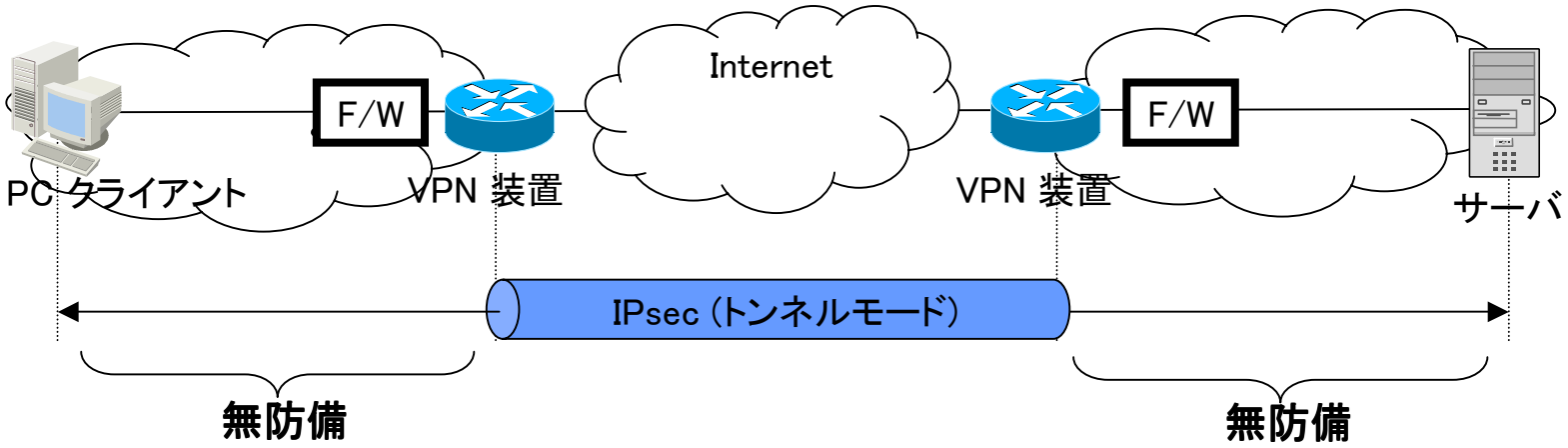
金庫モデル

IPsecのF/W越え（1）

HITACHI
Inspire the Next

＜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



しかし，－ 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)

HITACHI
Inspire the Next

＜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

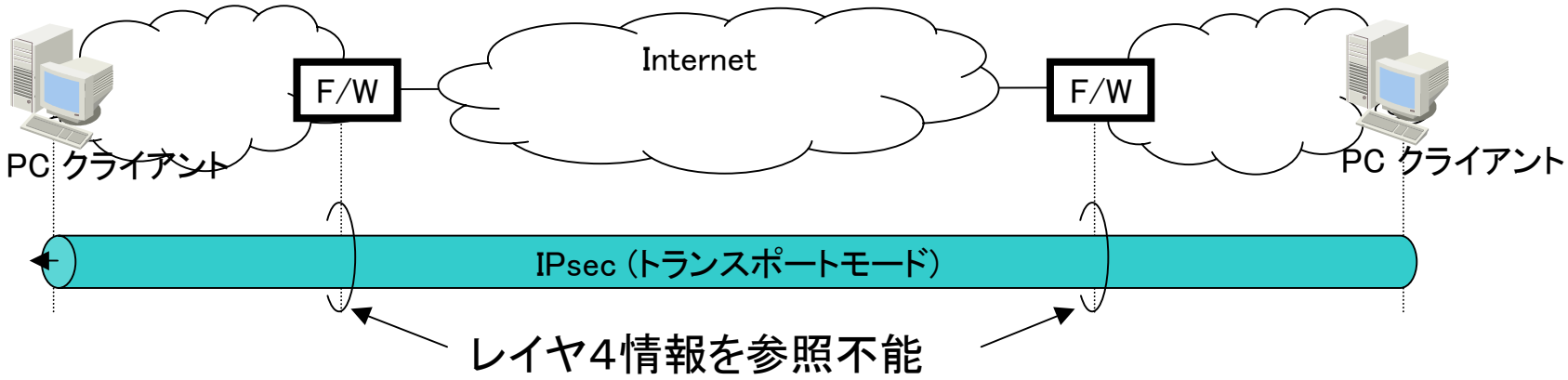
  →アプリケーションに依存することなく適用可能

  （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。

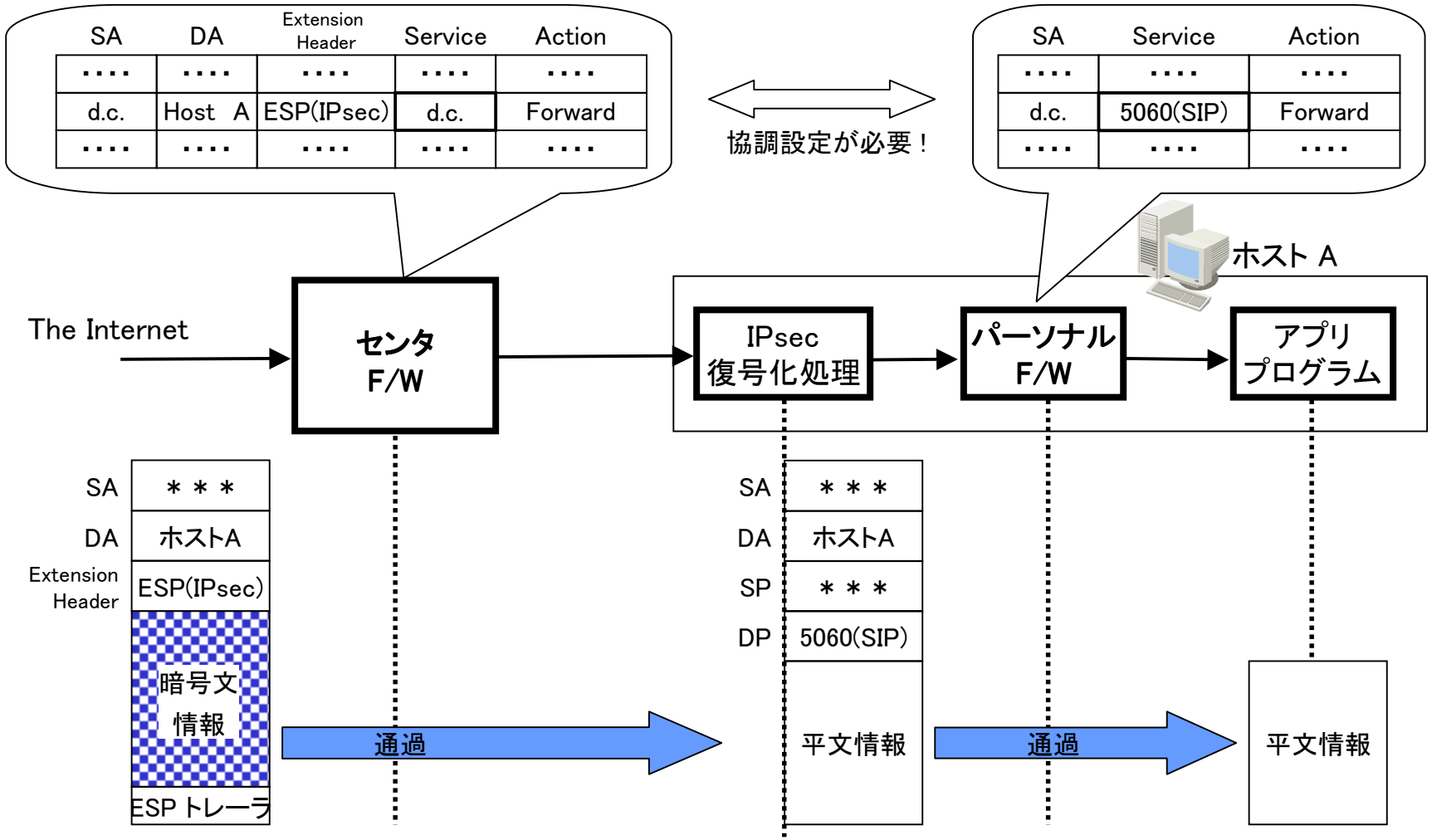
→新しいコンセプトのセキュリティモデルを導入する必要がある



IPsecのF/W越え（3）

HITACHI
Inspire the Next

＜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)

HITACHI
Inspire the Next

＜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 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

HITACHI
Inspire the Next

＜従来のF/W構成＞

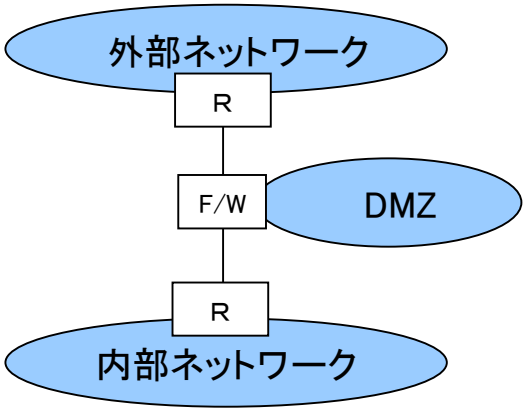
- F/Wが外部と内部を跨るアクセスを集中管理
- 通過するパケットは、F/Wが全数確認
- 公開サーバなどは、DMZに配置

＜問題点＞

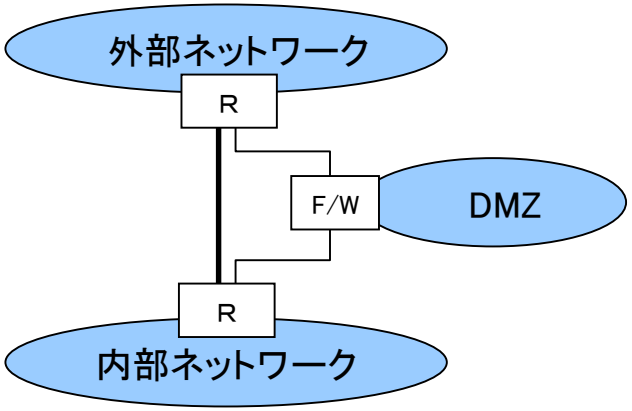
- ブロードバンド化に伴い、帯域的にF/Wがボトルネックになりつつある
- アプリケーションの多様化（P2Pアプリ、IPsec）

＜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。）



従来のF/W構成



将来のF/W構成

マルチホーム

HITACHI
Inspire the Next

＜マルチホームのメリット＞

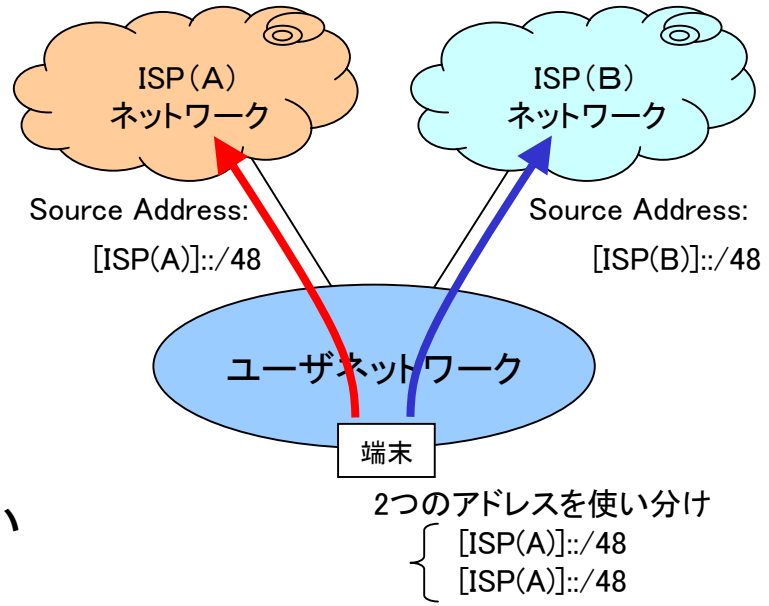
- インターネットへの接続に冗長性が確保される
- 経路最適化や負荷分散が設定可能

→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

企業内ネットワークアクセス制御

HITACHI
Inspire the Next

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

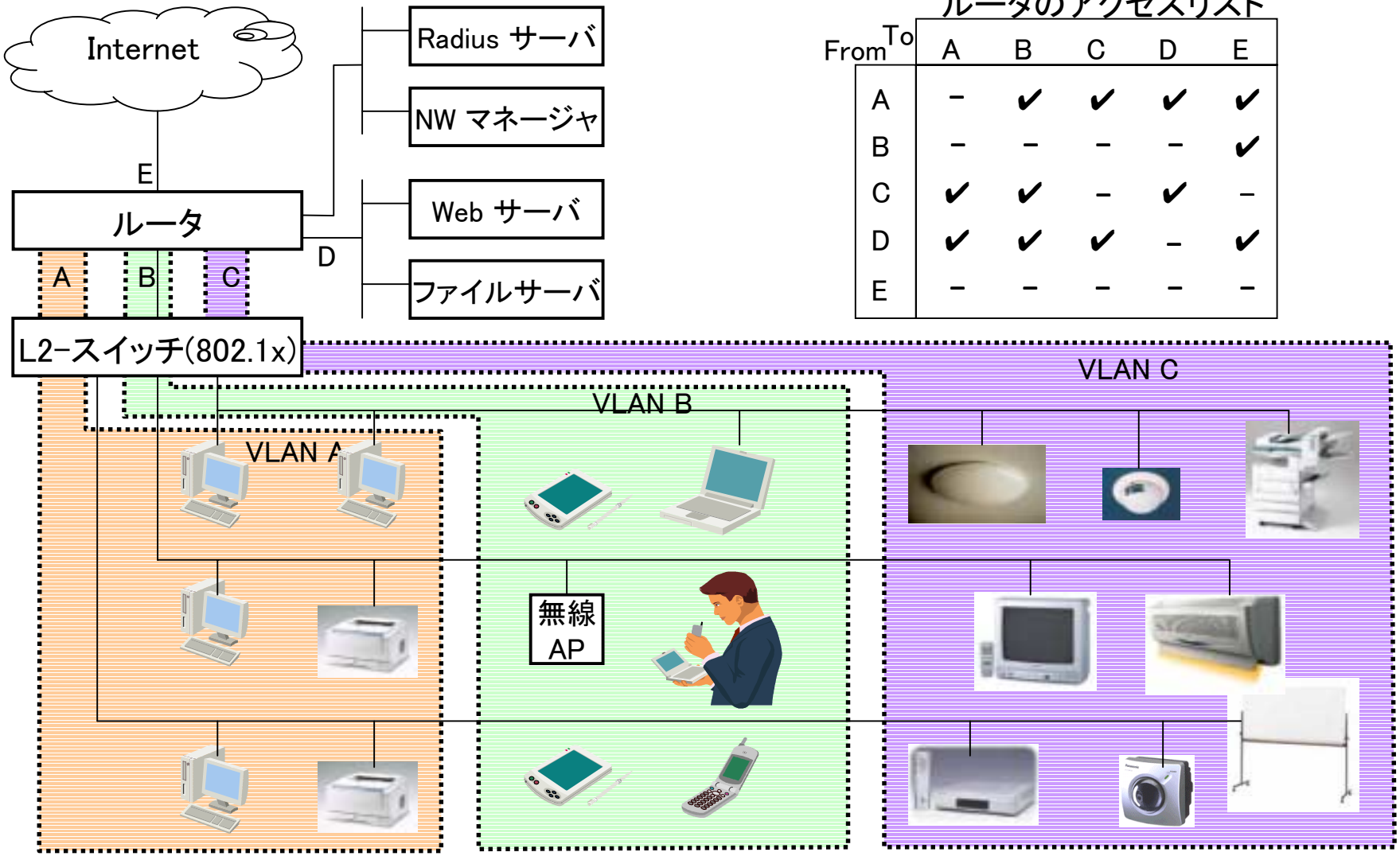
＜アクセスポリシーの例＞

- 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

企業内ネットワークアクセス制御

HITACHI
Inspire the Next

＜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	–	–	–	–	–

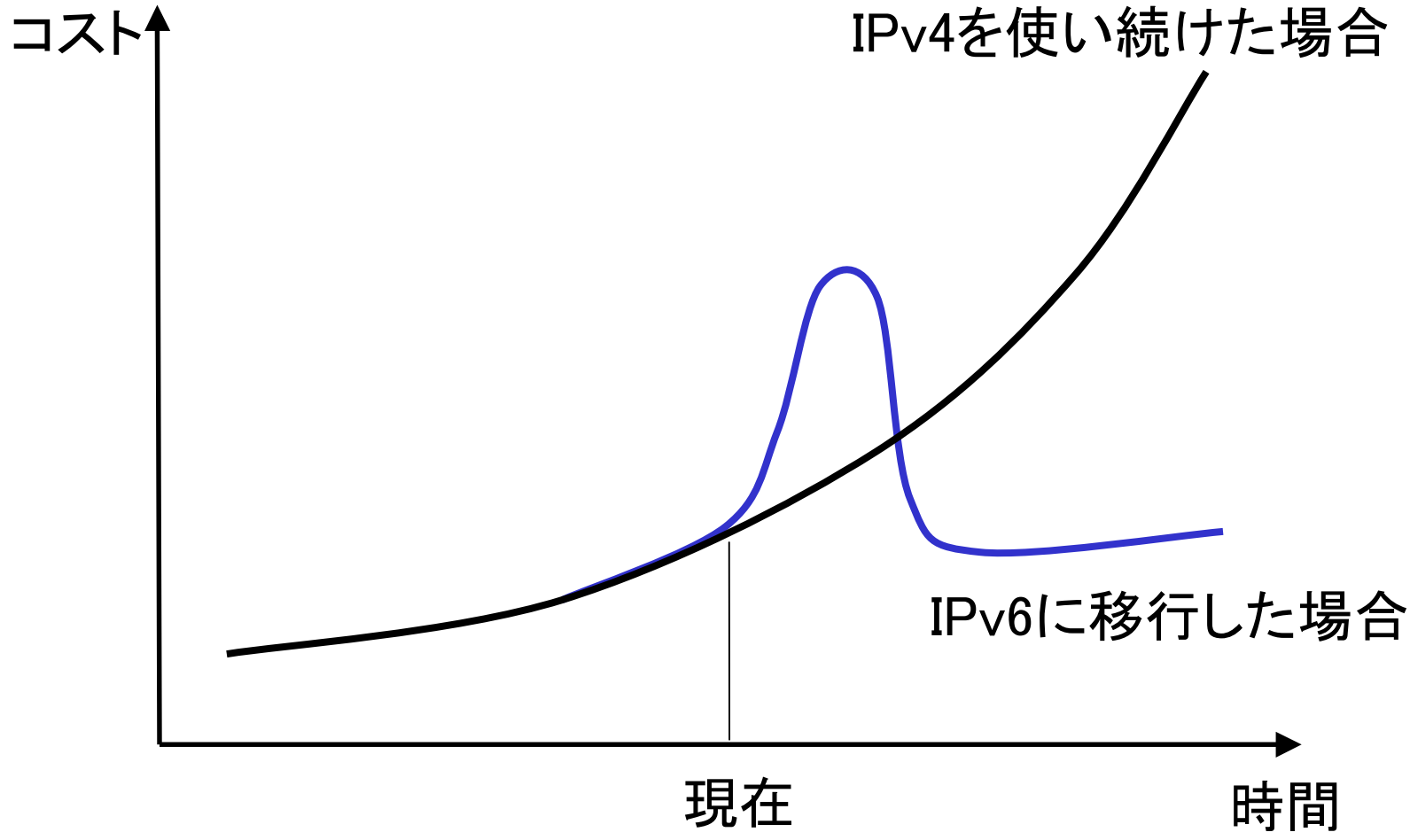
HITACHI
Inspire the Next

6

まとめ

IPv6導入の効果

HITACHI
Inspire the Next



まとめ

HITACHI
Inspire the Next

IPv6に対して、過剰に期待するのは危うい。

但し、IPv4で妥協するのはもっと危うい。

今こそ、IPv6移行の第一歩を踏み出す時期です。

P.S.　本資料作成にあたっては、IPv6普及･高度化推進協議会のIPv6移行WGのメンバの方々には、多大なるご協力を得ております。