エンタープライズネットワークへのIPv6導入

2004年12月1日

NEC
中原　一彦
nakahara@cq.jp.nec.com

Empowered by Innovation NEC

本パートでは、

- 移行や運用ノウハウ蓄積には時間がかかる

  IPv6活用へのバリア

(1) **やり方がわからない –移行ガイドラインの活用-**
アドレスの取得方法やアドレスの種類の選択、利用方法
セキュリティ対策の方法

(2) **製品・サービスの品質・安定度に不安がある –構築手法の工夫-**
既存ネットワークへの影響を与えない構築方法

(3) **メリットがみえない –ケーススタディ-**
端末間通信であるIP電話での活用, Multicastによる映像配信などで活用

- **IPv6導入を検討しているエンタープライズネットワーク管理者にむけて移行ガイドラインを適用させたケーススタディを紹介する。**

© NEC Corporation 2004

Empowered by Innovation NEC

目次

© NEC Corporation 2004

Empowered by Innovation NEC

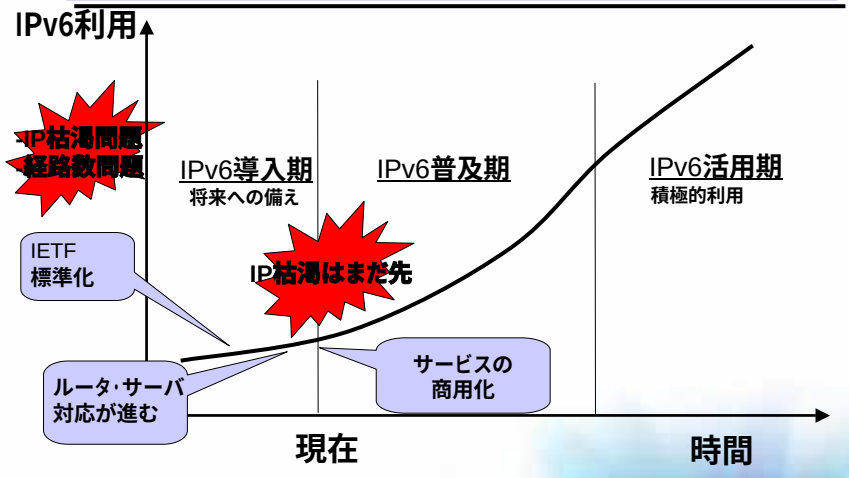
IPv6移行の現状

© NEC Corporation 2004

Empowered by Innovation NEC

現状認識

IPv6への移行の現状



現在IPv6導入期：普及期へのハザマでもっともエネルギーを要する時期

© NEC Corporation 2004

Empowered by Innovation NEC

サービス例

- IPv6によるマルチキャスト配信：BIGLOBE.TV
  http://bbtv.biglobe.ne.jp/4md/
  - 地上波，衛星，ケーブルTVに次ぐ、４つ目のメディアと位置づけ
    - NTT東のIPv6地域網を利用して、IPv6マルチキャストによる多チャンネル放送，映画ビデオ等のVoDサービスを提供
- IPv6電話サービス：BIGLOBE TVフォン[PN]
  http://phone.biglobe.ne.jp/tvphone/pn/
  - NTT東のIPv6地域網を利用した**新たなＩＰテレビ電話サービス**

IPv6網を利用したサービスは開始されている

© NEC Corporation 2004

Empowered by Innovation NEC

おさらい

IPv6の特長

柔軟なアドレス設計

(1) アドレス空間の拡大
シンプルなネットワークの実現
将来的にネットワーク端末の多様化に対応する拡張性

(2) 整理されたアドレッシングアーキテクチャ
ネットワークの再設計が可能

運用性向上

(3) Plug and Play (PnP)
エンドユーザ端末のサポートの負荷軽減に活用。

選択肢の多様化

(4) セキュリティの強化
エンドツゥエンドでのセキュリティの確保が可能。
(管理者はPnPで利用させるまでの手法の確立に課題)

(5) モバイルIP、マルチキャスト
新しいネットワーク利用形態に活用

(6) QoSの強化
最適なネットワーク品質の確保のための帯域制御の実現

Empowered by Innovation NEC

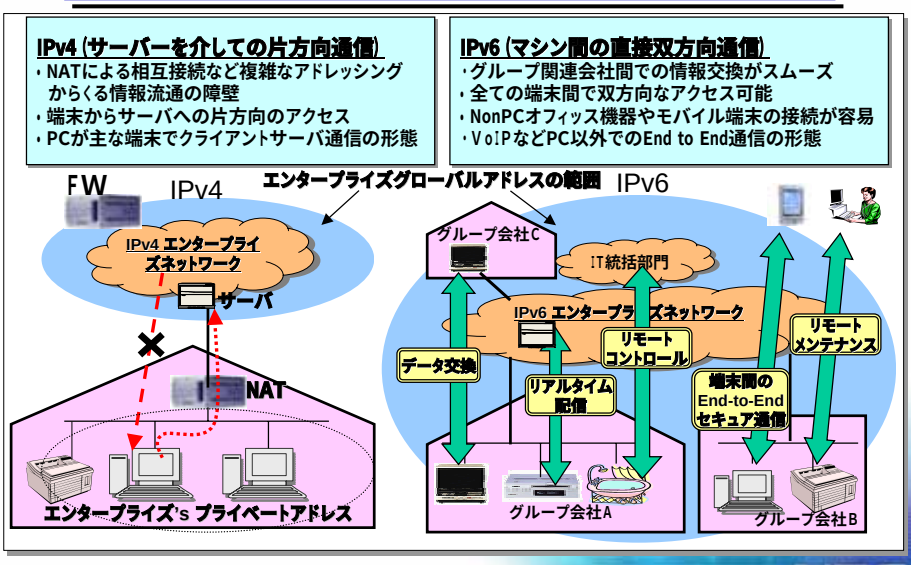
© NEC Corporation 2004

おさらい

IPv6の特長と変化(イメージ図)

IPv4 (サーバーを介しての片方向通信)
- NATによる相互接続など複雑なアドレッシングからくる情報流通の障壁
- 端末からサーバへの片方向のアクセス
- PCが主な端末でクライアントサーバ通信の形態

IPv6 (マシン間の直接双方向通信)
- グループ関連会社間での情報交換がスムーズ
- 全ての端末間で双方向なアクセス可能
- NonPCオフィス機器やモバイル端末の接続が容易
- VoIPなどPC以外でのEnd to End通信の形態



Empowered by Innovation NEC

© NEC Corporation 2004

IPv6を今導入する理由

⑴ 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

⑵ 新規アプリケーション（マルチキャスト/VoIPなど)導入に伴うIPv6導入
・出張、会議などの業務効率改善。ユビキタス化
・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の対応

⑶ IPv6開発のための環境整備
・IPv6関連製品の開発自体が目的

⑷ 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。
・ライバル会社の導入により、対抗的に導入。

出展: 2004年版「IPv6移行ガイドライン」(一部加工)

© NEC Corporation 2004

Empowered by Innovation NEC

IPv6移行技術の紹介

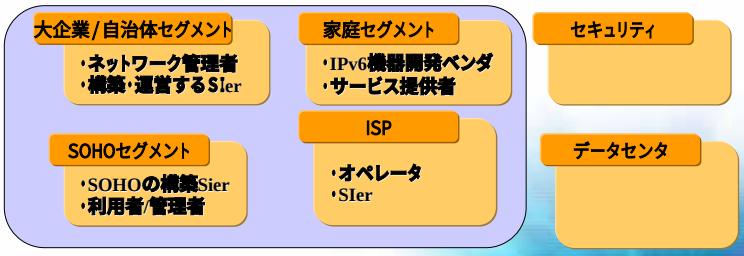
© NEC Corporation 2004

Empowered by Innovation NEC

移行ガイドライン

- IPv6普及・高度化推進協議会　移行WG
  - 郵政省(現総務省)をオブザーバに迎え、「IPv6による次世代インターネットの普及推進を目的とした協議会」の中の移行に関する分科会
- 移行ガイドライン
  - ４つのセグメントに分けて移行シナリオを検討しガイドラインを策定 (２００４年版)
  - ６つのセグメントに分けて移行シナリオを検討しガイドラインを改訂中

利用主体毎のガイドラインで移行プロセスが明らかに

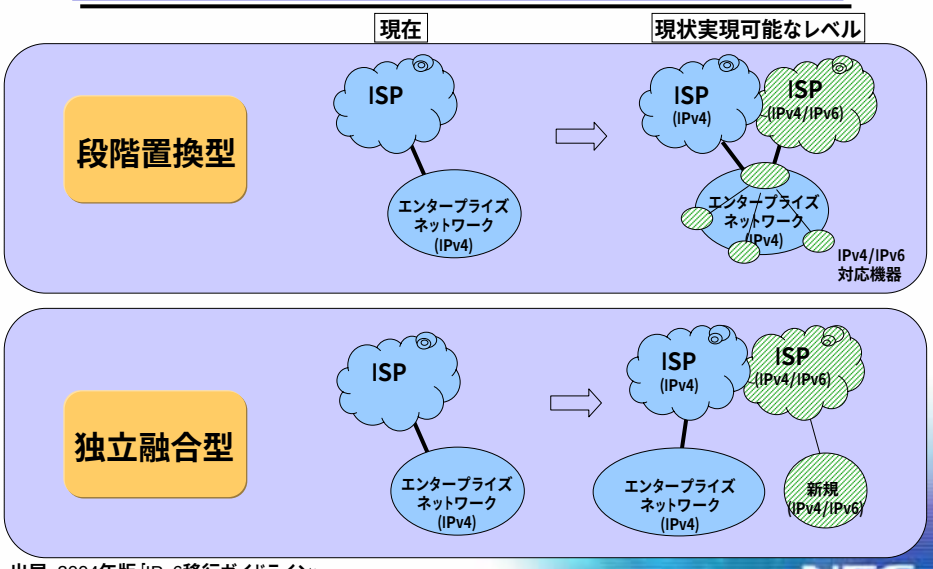


出展: http://www.v6pc.jp/jp/wg/transWG/index.html

© NEC Corporation 2004

Empowered by Innovation NEC

2種類の移行パターン

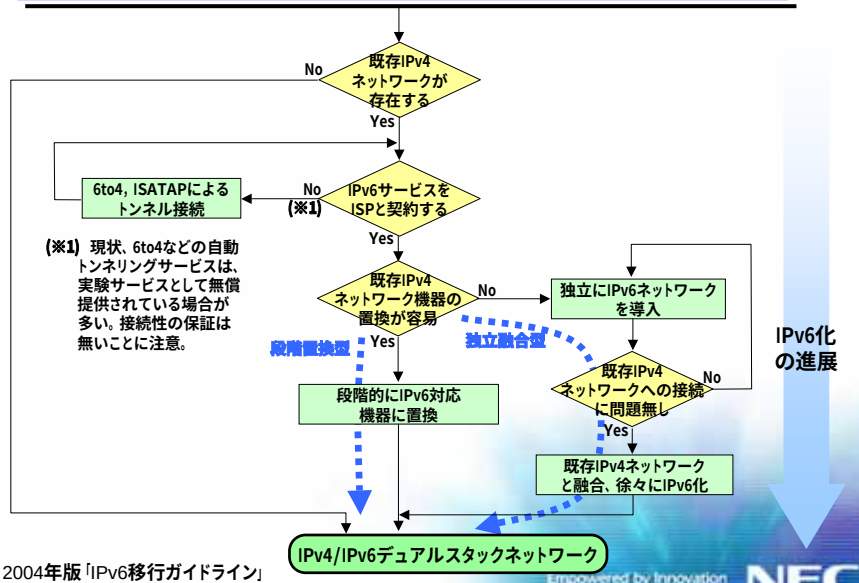


出展: 2004年版「IPv6移行ガイドライン」

© NEC Corporation 2004

Empowered by Innovation NEC

IPv6 ネットワーク構築のフロー

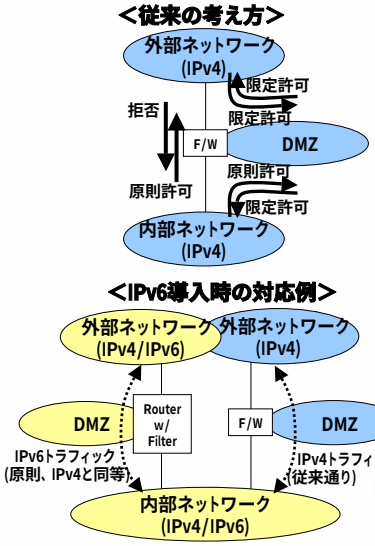


(※1) 現状、6to4などの自動トンネリングサービスは、実験サービスとして無償提供されている場合が多い。接続性の保証は無いことに注意。

出展: 2004年版「IPv6移行ガイドライン」

© NEC Corporation 2004

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
- ・NAT(アドレス変換)
- ・リモートアクセス
- ・ロギング
- ・ウィルスチェック
- ・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部分で処理する。

出展: 2004年版「IPv6移行ガイドライン」(一部加工)

© NEC Corporation 2004

クローズド網へのIPv6導入方法

© NEC Corporation 2004

クローズドへのIPv6導入

- *エンタープライズとは*
  - 独立してTCP/IPを利用してネットワークを運用している組織
  - 独立してネットワークのアドレッシング計画やアドレス割り当てを行う組織

  まずは、エンタープライズネットワークの外からのセキュリティ対策の負荷をかけない導入方法としてクローズド網から導入

- IPv6アドレス計画をどうするか
- IPv6網の接続をどうするか

© NEC Corporation 2004

IPv6アドレス(1)

＜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アドレスのISP-Freeな取得方法＞

- 適当にIPv6アドレスを割り当てる
- RFC２７４１のテストアドレス(3ffe)を取得し割り振り、割り当てる
- グローバルユニーク・ローカルアドレス (fc00::/7)を割り当てる

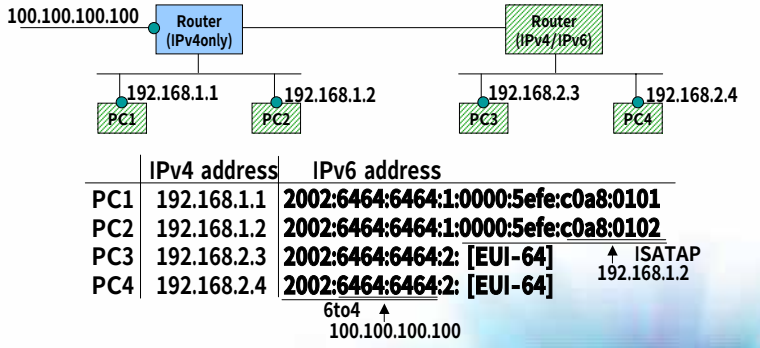
⇒ **実行には躊躇**

＜サイトローカルアドレス＞
RFC3871: サイトローカルアドレスの実装を禁止
→　利用すべきアドレスではない

© NEC Corporation 2004

IPv6アドレス(2)

- グローバルIPv4アドレスと6to4アドレス生成ルールを利用することでアドレス重複が発生しないことを考慮したIPv6アドレスが利用可能



出展: 2004年版「IPv6移行ガイドライン」

© NEC Corporation 2004

IPv6アドレス(3)

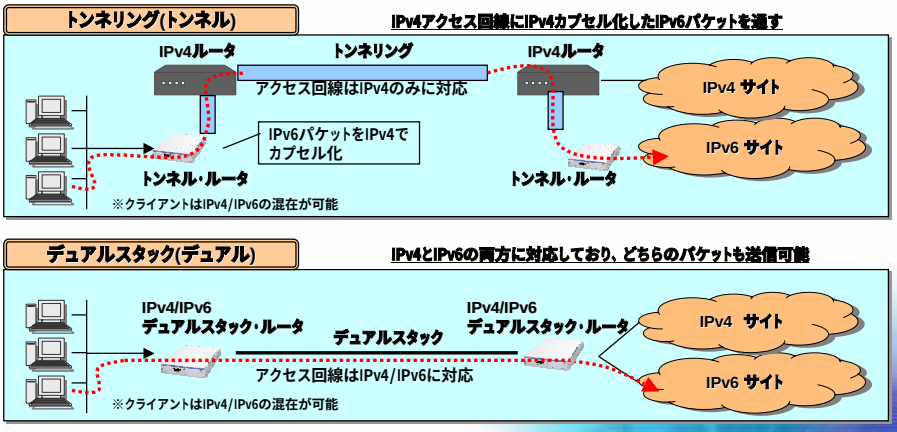
- /32を取得するには、以下のポリシーに準ずる必要がある
  - be an LIR;
    - LIRとなること、つまりアドレス割り当てと管理を行う
  - not be an end site;
    - エンドサイトではない 、つまりアドレスを割り当ててもらう側ではない
  - plan to provide IPv6 connectivity to organizations to which it will assign /48s, by advertising that connectivity through its single aggregated address allocation;
    - /48を割り当ている組織体にIPv6の接続性を提供し、その経路を集約し広告する計画があること
  - have a plan for making at least 200 /48 assignments to other organizations within two years.
    - ２年以内に他の組織体へ少なくとも/48を200サイトへ割り当てる計画があること
- また、IPv6割り振りガイドラインでは、
  - A large organization providing IPv6 connectivity to its group companies or subsidiaries and restricting connectivity to its own network
    - IPv6の接続性をグループ会社か、子会社へ提供し、自営網への接続性を制限する大組織体

© NEC Corporation 2004

Empowered by Innovation NEC

サイト間の接続(1)

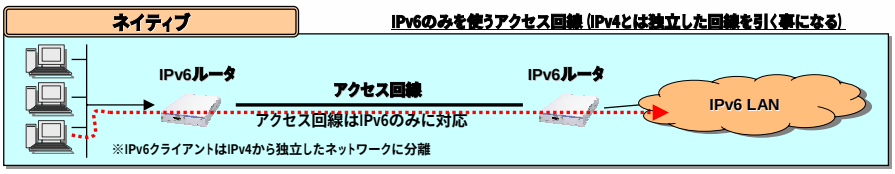
IPv6サービスの種類：既存のIPv4ネットワークとどう共存させるかにより、3種類に分類される。



© NEC Corporation 2004

Empowered by Innovation NEC

サイト間接続(2)

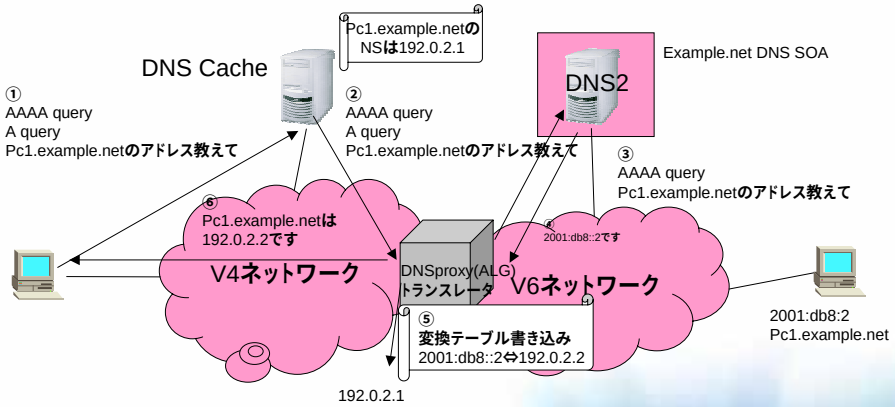


エンドトゥエンド通信の場合		宛先		
		IPv4シングルスタック搭載	IPv6/IPv4デュアルスタック	IPv6シングルスタック搭載
送信元	IPv4シングルスタック搭載	○(IPv4で通信)	○(IPv4で通信)	×(通信不能)
	IPv6/IPv4デュアルスタック	○(IPv4で通信)	○(IPv6で通信)	○(IPv6で通信)
	IPv6シングルスタック	×(通信不能)	○(IPv6で通信)	○(IPv6で通信)

© NEC Corporation 2004

Empowered by Innovation NEC

IPv6/IPv4トランスレータとは

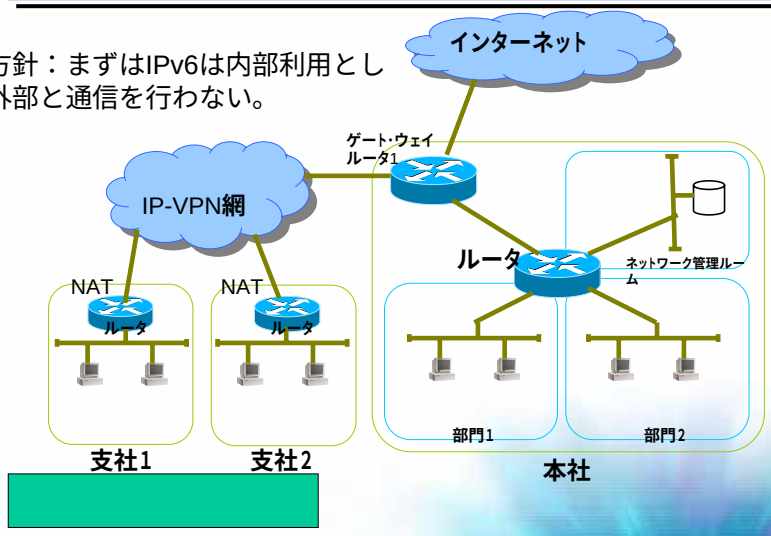


© NEC Corporation 2004

Empowered by Innovation NEC

エンタープライズ網移行のイメージ

方針：まずはIPv6は内部利用とし
外部と通信を行わない。

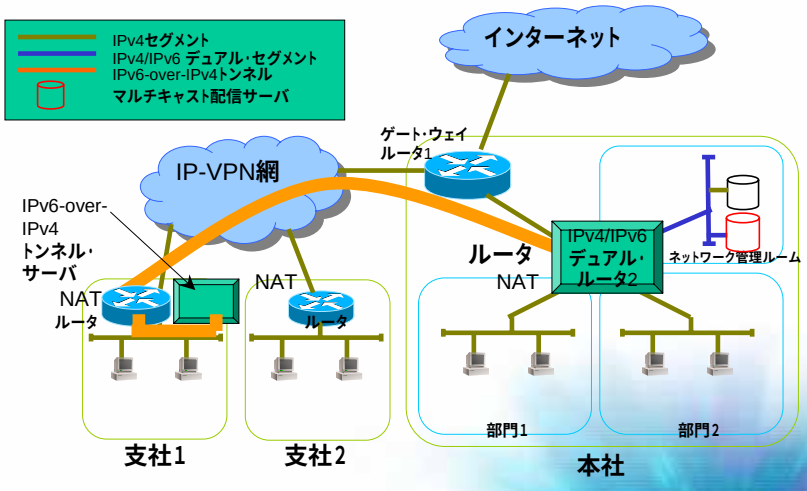


出展: http://www.ipv6style.jp/jp/index.shtml IPv6虎の巻(一部加工)

© NEC Corporation 2004

Empowered by Innovation NEC

エンタープライズ網IPv6 over IPv4のイメージ



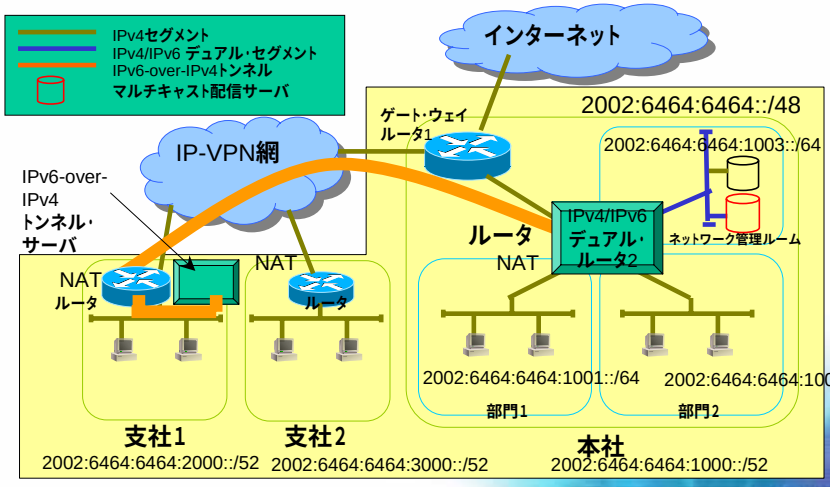
出展: http://www.ipv6style.jp/jp/index.shtml IPv6虎の巻(一部加工)

© NEC Corporation 2004

Empowered by Innovation NEC

エンタープライズ網アドレッシングのイメージ

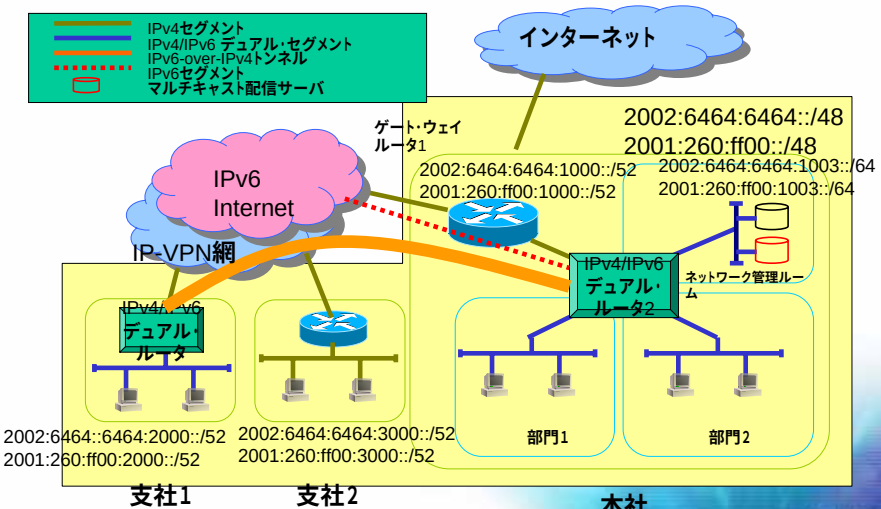
ここでは、内部のIPv4アドレスからユニークなIPv6アドレスを生成し利用
IPv4がワールドでユニークならIPv6もワールドでユニークになる。



出展: http://www.ipv6style.jp/jp/index.shtml IPv6虎の巻(一部加工)

© NEC Corporation 2004

エンタープライズ網の対外接続時イメージ

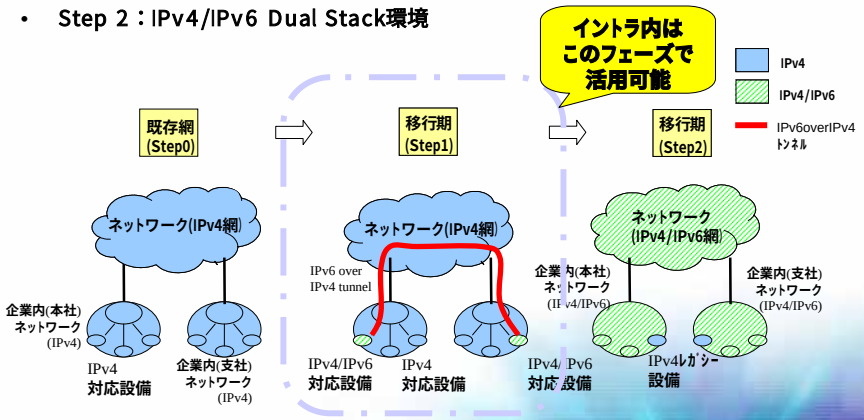


出展: http://www.ipv6style.jp/jp/index.shtml IPv6虎の巻(一部加工)

© NEC Corporation 2004

IPv6移行方法例 (段階置換型)

- Step 0：既存網（IPv4のみ）
- Step 1：IPv6アイランドが点在し、IPv4トンネルで接続
- Step 2：IPv4/IPv6 Dual Stack環境



© NEC Corporation 2004

Empowered by Innovation NEC

IPv6活用にむけたケーススタディ

© NEC Corporation 2004

Empowered by Innovation NEC

企業ネットワークへのIPv6導入動機

エンタープライズネットワークの代表的ネットワーク
企業網での導入動機

導入メリットの明確化	-管理コストの削減 -通信能力の向上 -管理内容の充実
How-Toの明確化	-作業負荷、投資額はどのくらいか -何を調達し、何をどういう順番で 変更していくべきか
変化の明確化	-何が変わって何がかわらないかの明確化

Empowered by Innovation NEC

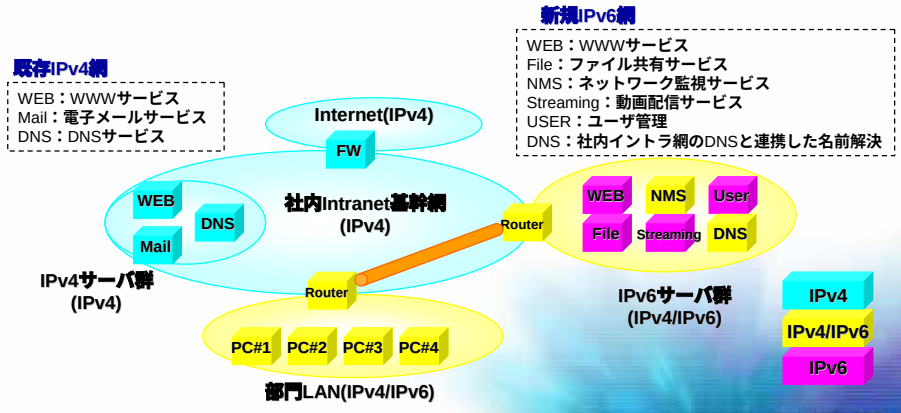
アプリケーション

- WWW
  - 本プロジェクト情報発信用WEB。
    - 文字/画像の他に、動画をマルチキャストにより配信
- ファイル共有
  - WebDAVにより、プロジェクトの情報共有を実施。 ✔
- ストリーミング配信
  - 動画コンテンツを、マルチキャストを用いて帯域を有効活用して配信 ✔
- リモートアクセス
  - IPv6 over IPv4トンネルをIPsecクライアントを用いてリモートアクセスを実現
- IP電話
  - SIPを用いたVoIPを実現 ✔
- TV会議
  - 遠隔拠点間のTV会議を実現
- ネットワーク監視
  - 既存IPv4網とIPv6網を共存させるため、既存網への影響が出ないことを、トラフィック監視により実行。
    - Snmpを用いて、IPV6-MIB情報を取得
- ユーザ管理
  - IPv6ユーザの情報(特にIPv6アドレス)を、一元的な管理の実施

Empowered by Innovation NEC

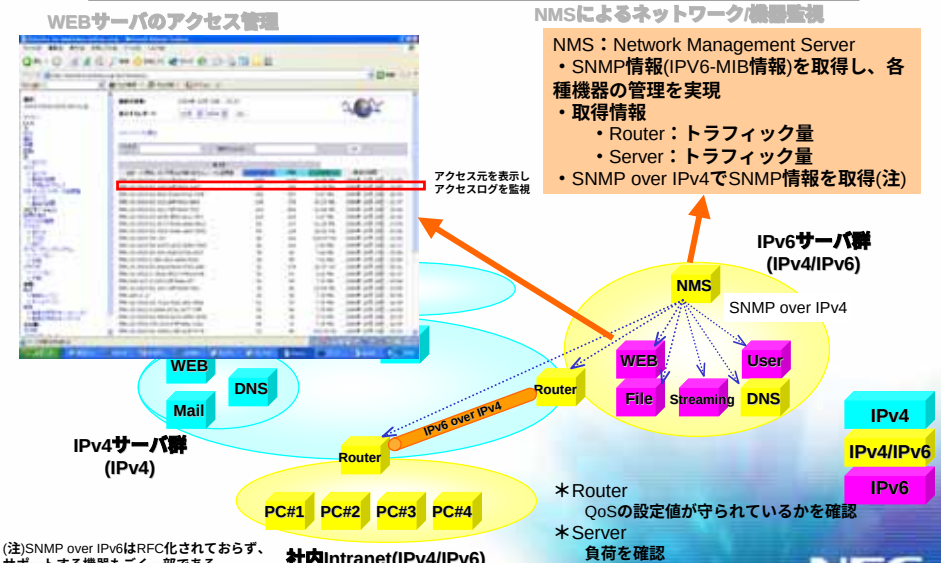
ネットワークイメージ

- 既存のIPv4網に影響を与えないIPv6網の構築方法
  - IPv6網はIPv6 over IPv4トンネルで構築
  - IPv6サービス(ファイル共有、ストリーミング、PtoP通信 etc…)を追加



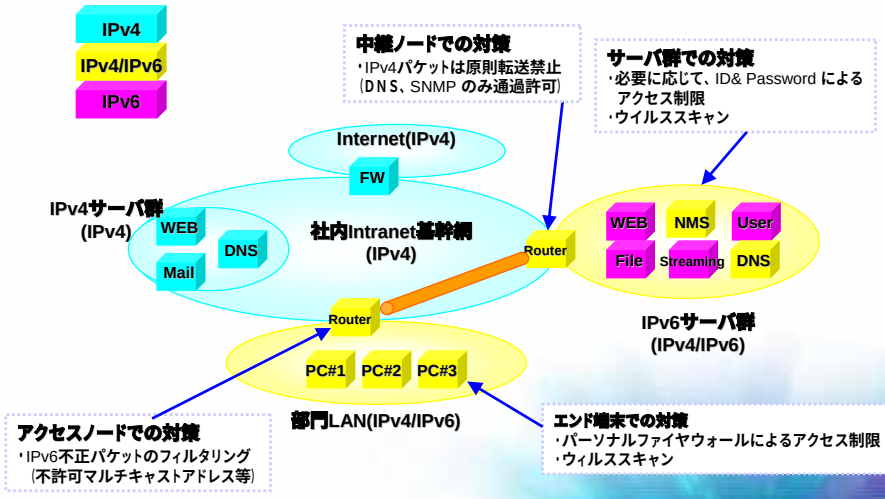
© NEC Corporation 2004

ネットワーク監視



© NEC Corporation 2004

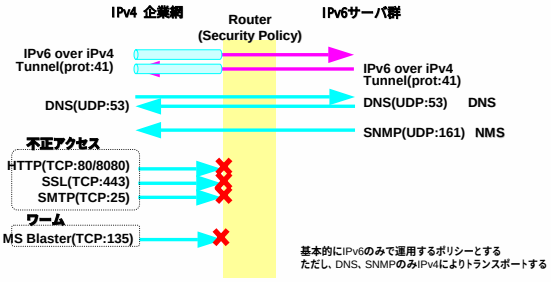
セキュリティ方針例

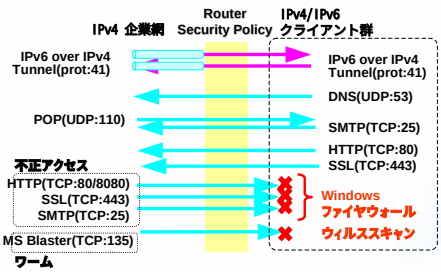


パケットフィルタリングモデル

サーバセグメント

- 基本的に、IPv6のみで運用を行なうことで、IPv4に対する影響、もしくはIPv4に対する影響を排除
- IPv6でトランスポートできないプロトコル（WindowsにおけるDNS、SNMP等）はIPv4で転送
- IPv4でサービス済みのサービスはIPv6化しない





IPv6/IPv4クライアント群

- 既存サービス(E-mail、WEB等)はIPv4を用いて行なう。そのため、IPv4に対するフィルタリングは変更なし
- IPv6網にドメイン名でアクセスする場合、DNSサーバは既存DNSサーバを経由して行なう
- IPv6のフィルタリングは、原則として行わない
- 不正アクセス、ワーム等に対する対策は、各端末におけるパーソナルファイアウォールにて行なう。

端末管理

・アドレス管理／アクセス管理／設定情報(DNS情報)の提供について

	端末へのアドレス設定	DNSサーバへのアドレス登録
IPv4	Static設定/DHCP	Staticが一般的
IPv6	RA/Static設定	Endノードの登録は？

・IPv4では、DHCPのログから端末を特定することが可能である
・IPv6では、RAによるアドレス設定を採用した場合、アドレス取得時のログや認証が難しいため、ある期間のアクティブユーザの特定が難しい。インターフェース識別子に含まれるMACアドレスで管理したとしてもRAで端末管理は現状完　全ではない。(802.1xのようなL2レベルでの管理が必要)

出展: 2004年版「IPv6移行ガイドライン」(一部加工)

© NEC Corporation 2004

Empowered by Innovation NEC

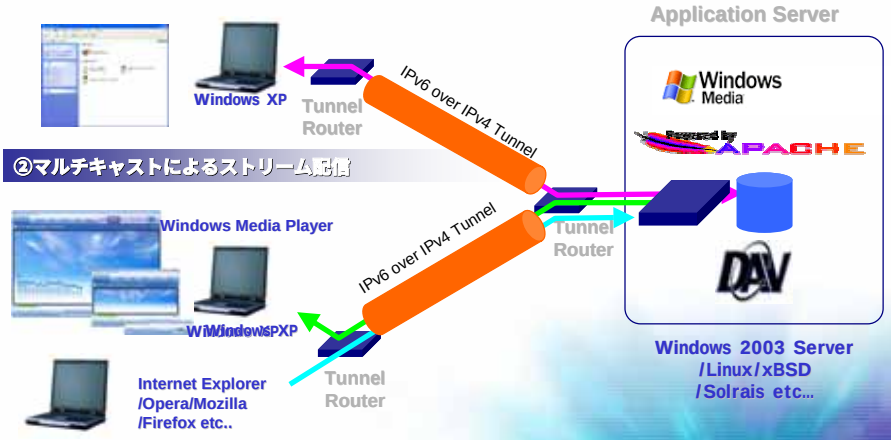
IPv6導入期に何が変わるか

- Plug&Playの出現
  - 同一リンク上の不正対策が必要となる。
    - 認証ＶＬＡＮの活用
    - ＲＡうっかり送信の対策としてpreference設定で防ぐ
- エンドツゥエンド通信　（IPSecなど活用）
  - サイト境界での検閲などが困難となる。テンポラリーアドレスを利用していた場合ロギングでの利用者特定が困難

© NEC Corporation 2004

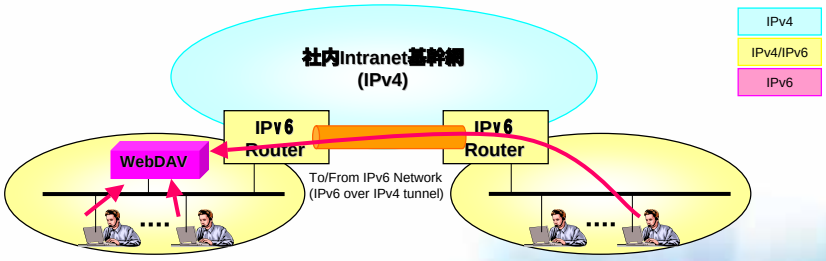
Empowered by Innovation NEC

アプリケーション例



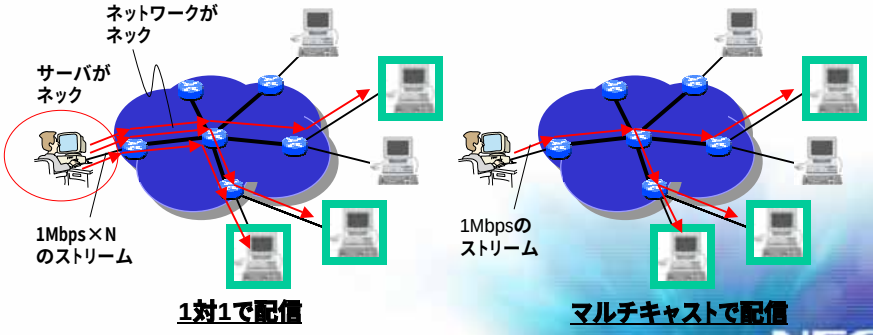
①ファイル共有サービス

- 部門横断的プロジェクトにて、情報共有を容易に実現
  - 部門間F/Wの設定変更を必要とせず、管理・運用コストの削減とad-hoc的なプロジェクトに迅速対応



②マルチキャストによるストリーミング配信

- 特にマルチキャストの活用においてIPv6がお勧め
  - 受信クライアントが増加してもトラヒックは増加しない
  - サーバの負荷を軽減できる
  - キャッシュ/負荷分散という手もあるが、
  - リアルタイムのストリーム配信にマルチキャストが効果絶大

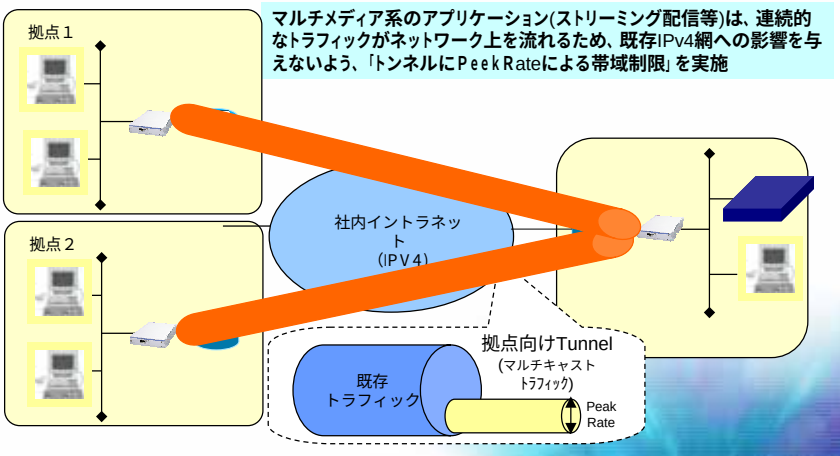


© NEC Corporation 2004

Empowered by Innovation NEC

利用帯域の制御について

- マルチキャスト対応バックボーン構築にはコストがかかるためこれから構築する場合、必要なところのみに配送するための構築の場合、トンネリングが有効



© NEC Corporation 2004

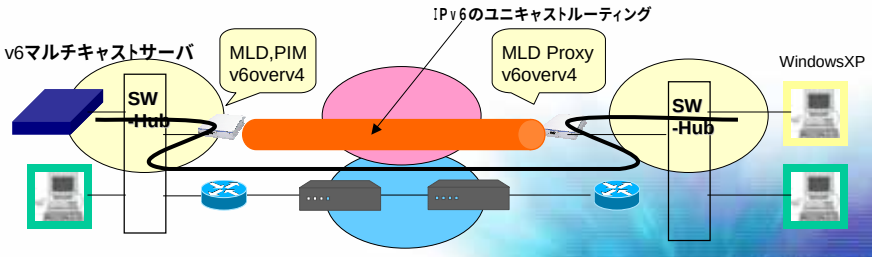
Empowered by Innovation NEC

ソリューション比較(IPv6 over IPv4)

なぜIPv6？

- IPv6マルチキャスト対応バックボーンを構築するにはコストが発生する。
- しかし、アクセス網でIPv4マルチキャスト対応しているケースは極まれ

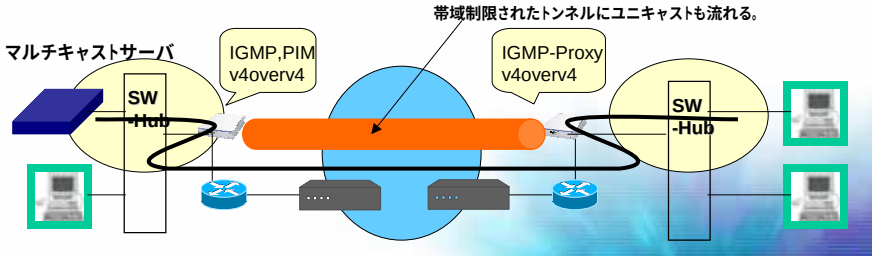
  (答え) マルチキャストoverIPv4トンネルで必要なサイトのネットワークへマルチキャストを配信する
  - Multicast(IPv6)とUnicast(IPv4)の分離(帯域の制御)が可能
    - 運用ポロシーを分離して管理が可能
    - IPv6/IPv4の相互の経路設計が容易



© NEC Corporation 2004

ソリューション比較(IPv4 over IPv4)

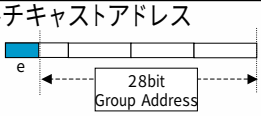
- IPv4マルチキャスト対応バックボーンを構築するにはコストが発生する。
  - IPv４マルチキャストoverＩＰｖ４トンネルで必要なネットワークへマルチキャストを配信すると、
    - MulticastとUnicastの分離がされず帯域コントロールが難しい
      - 回避する方法としてはVLANで分割しMulticast用セグメントのユニキャストルーティングの設定
      - トンネルインターフェースへマルチキャストのみがながれるようにユニキャストルーティングを設定



© NEC Corporation 2004

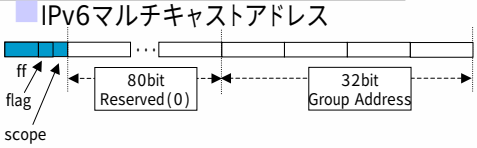
IGMP Snoopingについて

IPv4マルチキャストアドレス



- RFC3171(IANA予約アドレス)
  - ・244.0.0.1 All Systems on this Subnet
  - ・244.0.0.2 All Routers on this Subnet
  - ・232/8 Source-Specific Multicast (SSM)
  - ・233.0.0.0～233.255.255.255(233/8)GLOP Block

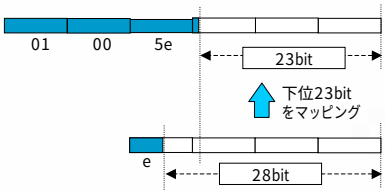
IPv6マルチキャストアドレス



- RFC2375(IANA予約アドレス)
  - ・FF02:0:0:0:0:0:0:1 All Systems on this Subnet
  - ・FF02:0:0:0:0:0:0:2 All Routers on this Subnet
  - ・FF0X:0:0:0:0:0:0:101 Network Time Protocol(NTP)

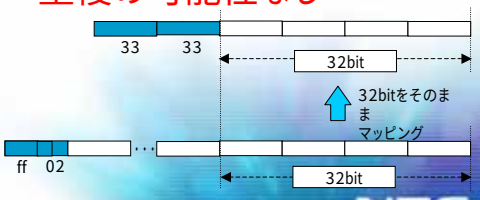
MACアドレス

重複の可能性あり



MACアドレス

重複の可能性なし



Empowered by Innovation NEC

© NEC Corporation 2004

事例紹介

Empowered by Innovation NEC

© NEC Corporation 2004

IP電話でのIPv6活用

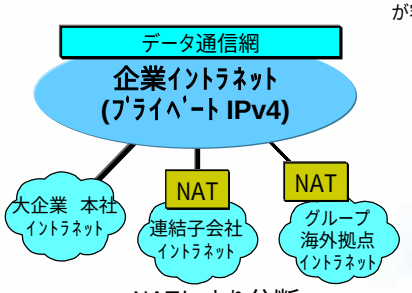
© NEC Corporation 2004

Empowered by Innovation NEC

IPv6化による企業網のメリット

【現状】
- NATにより、ｲﾝﾄﾗﾈｯﾄがｼｰﾑﾚｽでない
- 各セグメントへの端末収容は254台まで

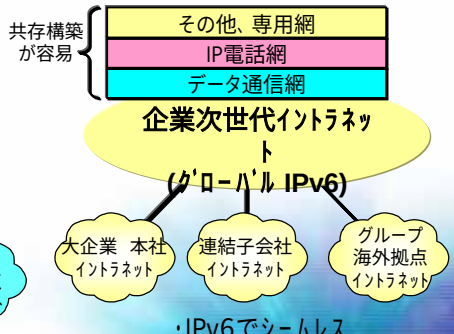
→IP端末増加に追従不可？



・NATにより分断

【IPv6化】
- IPv6により、ｼｰﾑﾚｽなﾈｯﾄﾜｰｸの構築が可能
- 収容端末数は実質的に無制限

→IP電話の導入等が容易



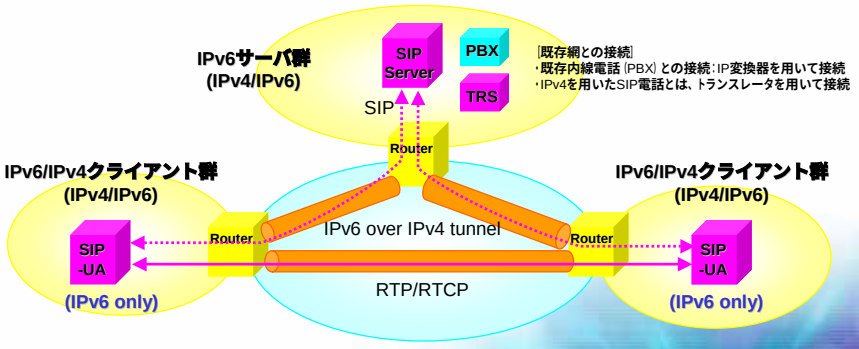
・IPv6でシームレス

© NEC Corporation 2004

Empowered by Innovation NEC

IP電話でのIPv6活用メリット

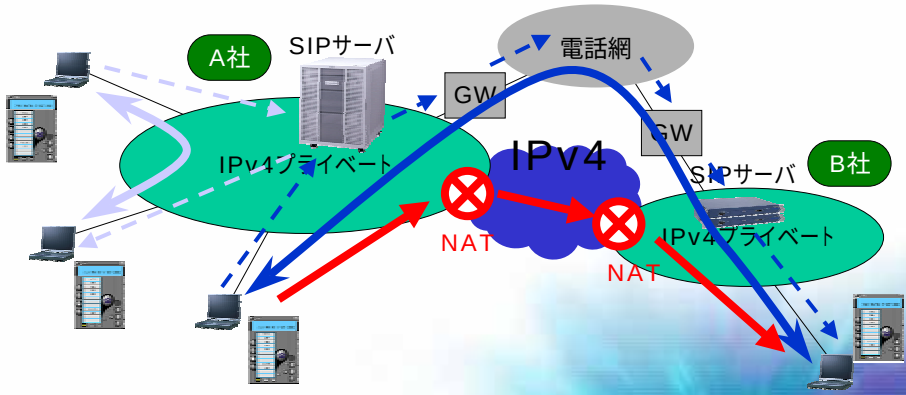
- グローバルなIPv6アドレスを付与することにより、NATを介さないPtoP通信を実現。また、企業網内部だけではなく、外部ともシームレスにアクセスすることが可能
- SIPサーバと組み合わせることにより、電話以外のサービス(プレゼンス情報など)を提供可能



© NEC Corporation 2004

現状のIP電話ネットワーク

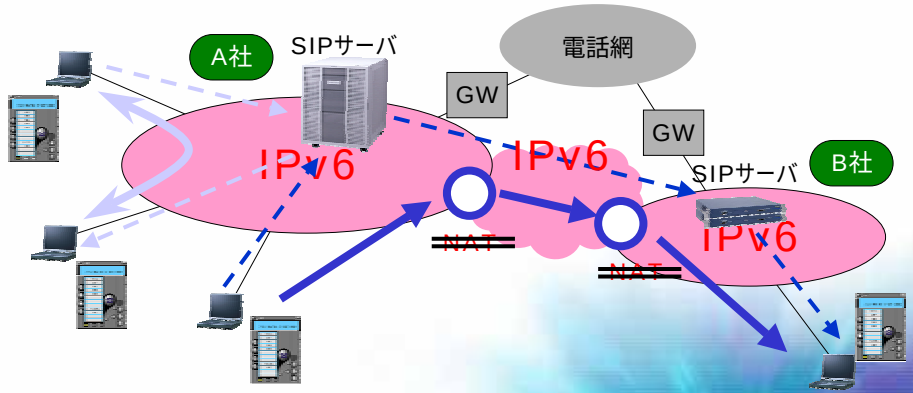
- 企業内でIPv4プライベートアドレスを使っていると企業間の接続はすべて既存電話網経由となる



© NEC Corporation 2004

IPv6活用時のIP電話ネットワーク

- IP電話はもっとも一般的なP2Pアプリケーション
- IPv6にすれば誰とでも、ダイレクトにP2P通信



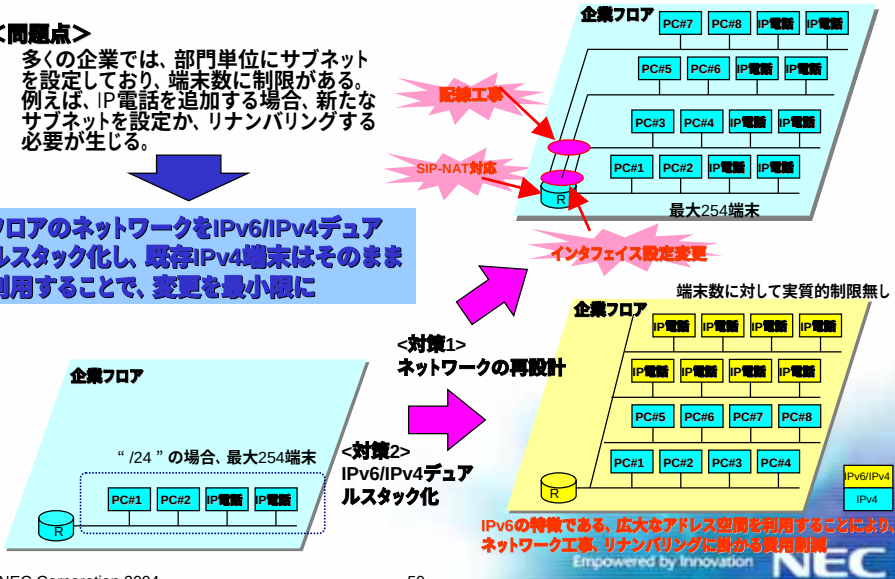
© NEC Corporation 2004

ソリューション(IP電話)

＜問題点＞

- 多くの企業では、部門単位にサブネットを設定しており、端末数に制限がある。例えば、IP電話を追加する場合、新たなサブネットを設定か、リナンバリングする必要が生じる。

フロアのネットワークをIPv6/IPv4デュアルスタック化し、既存IPv4端末はそのまま利用することで、変更を最小限に



© NEC Corporation 2004

ソリューションの比較

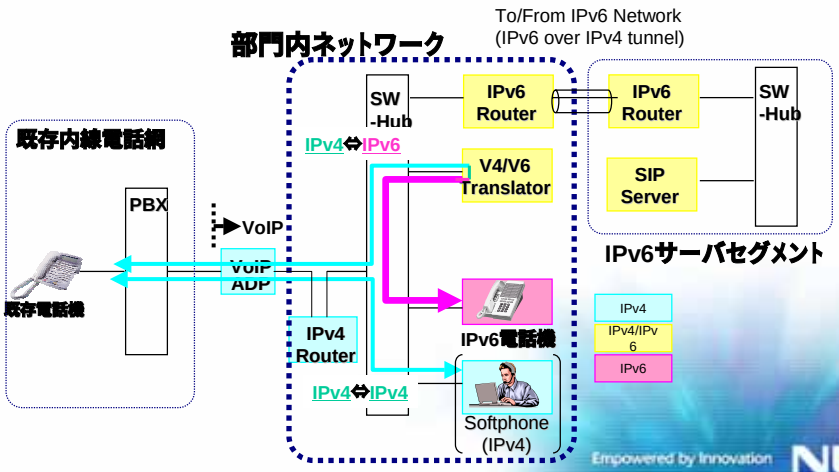
	方法	メリット	デメリット
IPv4	SIP-NAT	NAT装置を設置。またはルータにNAT機能をさせることで対応できる	NATより先のネットワーク状況が把握しにくく、複雑なネットワークになる 運用対象機器の増加を伴う 今後導入するアプリによっては、再度ネットワークの再設計が発生する可能性がある
	Renumber	再構築することで、管理しやすいネットワークを再設計できる	ネットワークの再設定作業や移行作業に時間とコストが発生。 今後導入するアプリによっては、再度ネットワークの再設計が発生する可能性がある
	ネットマスクを変更	Renumberしたときと同じような現象になる	
	セカンダリアドレス	その場限りの対応となりゆくゆくはいきづまりネットワークに	
IPv6	アドレス取得	端末増加に対応でき、ネットワークにscalabilityを持たせることができる。簡素なネットワークの構築が可能	IPv6対応のネットワーク構築が必要になる。

© NEC Corporation 2004

Empowered by Innovation NEC

移行時期のトランスレータの利用について

– IPv6電話-IPv6電話、 IPv4電話-IPv6電話、既存電話-IPv6電話の通話が可能
※ＩＰｖ６への移行過程を想定したネットワーク構成例



© NEC Corporation 2004

Empowered by Innovation NEC

IPv6活用にむけての考察

- 企業内での部門統合/分離や、M&Aによる事業規模の拡大等で、ネットワークもその変化に対応する必要がある
  - PCだけでなく、今後予想される情報端末(IP電話/放送受信機)導入等による端末の増加
  - IPv4で構築されたプライベートアドレスが、企業統合で生じるプライベートアドレスの重複(部門毎にNATなどを設置するケースもある)

IPv4を利用しつづけた場合ポイントソリューションとなり、その場対応の構築は、設計コスト・運用コストが継続的に発生してしまう可能性がある。

- P2Pアプリケーションの導入
- 既存ネットワークへのインパクトのなるアプリケーションの導入

シンプルで現在のIPv4ネットワークに影響が少なく、新規アプリケーションの追加に対応する最適なネットワークが必要
→ まずは、Firewall内部でIPv6でネットワークの最適化

© NEC Corporation 2004

Empowered by Innovation NEC

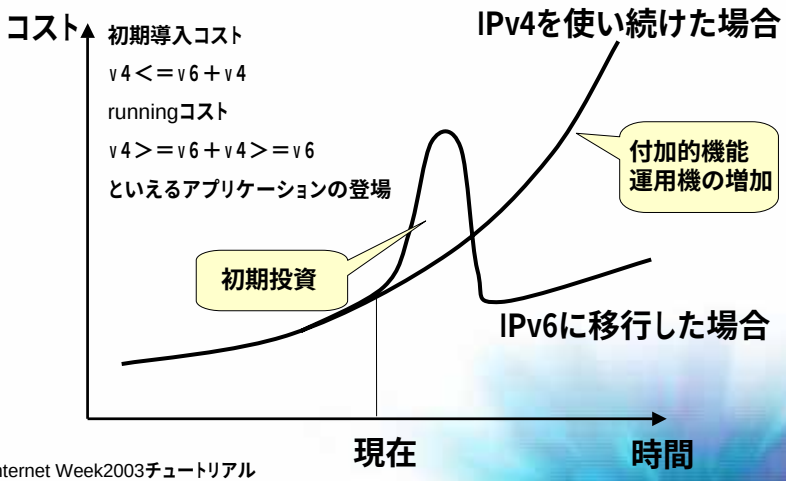
移行する際の懸念事項

- やはりIPｖ６アドレスをどのように入手するか！！
  - 本格的な導入ではＩＳＰのIPv6の接続サービスを購入で問題にはならない
  - Trial的な導入ではなお課題
- IPv6の対応で、ネットワーク機器のリプレースでコストが上がる？
  - 本格的な導入(バックボーン全体の対応)となると問題となる可能性がある。（SI費や設計費やらも?）
  - Trial的な導入では必要な部門/拠点にのみIPv6 over IPv4で対応することでインパクトは低いと考えられる。
- 全社に影響があるシステムへの影響は？
  - IPv4からの影響を排除するにはclosed網からの利用
  - 特にアプリケーション限定でIPv6を導入
  - ただし、アドレッシングに関してしっかりとした方針が必要かもしれない（内部経路の爆発を抑える対策）
- オペレーションが２倍になるのでは！
  - シンプルなネットワーク構築を実践することが重要。
  - 設計の仕方しだいでは、単純に２倍とはならないはず。

© NEC Corporation 2004

Empowered by Innovation NEC

IPv6導入効果



出展:Internet Week2003チュートリアル
「企業におけるIPv6ネットワーク利用」(一部加工)

© NEC Corporation 2004

まとめ

- ケーススタディから、新規のアプリケーションを導入する際、構築済みのネットワークを再設計が必要という問題を示した。
- 代表的な問題はアドレスの重複問題や、端末数の増加等によるアドレス割り当てやアドレッシング設計の行き詰まりの危機。マルチメディア系アプリケーションでは帯域コントロールも重要となる。
- IPv4で構築も可能であるが、追加機能や追加のネットワークトポロジー変更などの投資が必要であり、スケーラビリティや運用費を考えると将来性のあるIPv6の活用も選択肢に入る。
- まずは小さな規模からでも、IPv6を活用しIPv4の業務ネットワークと共存したネットワークを設計してみてはいかがだろうか。

© NEC Corporation 2004

ご質問は？

© NEC Corporation 2004

Empowered by Innovation

NEC

ご清聴ありがとうございました。