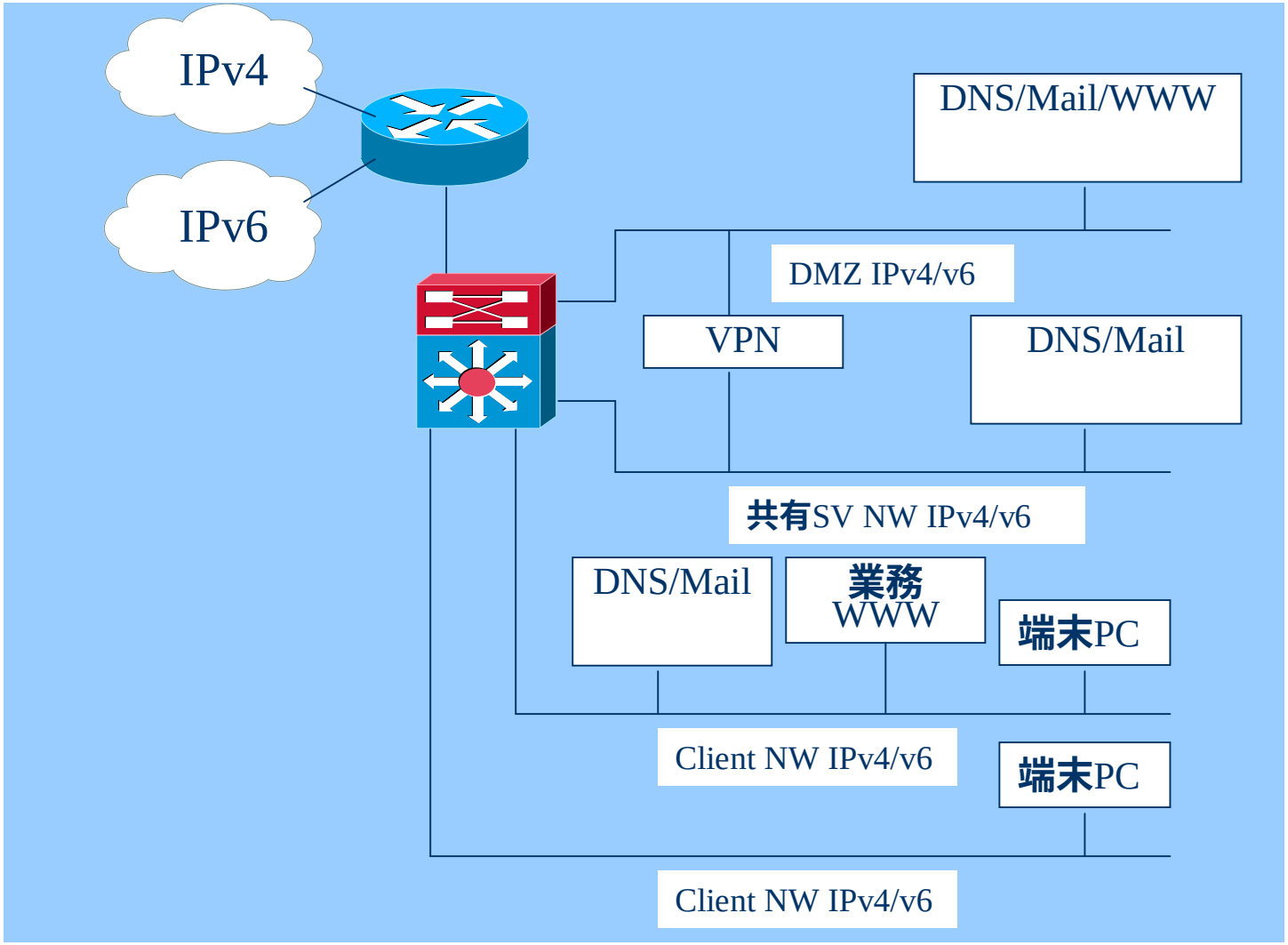
企業ネットワークをIPv6で統一した際の移行方法と課題

久保　孝弘
株式会社KDDI研究所

KDDI R&D LABS

IPv6 専用網以前のNW構成 1/2



KDDI R&D LABS

IPv6 専用網以前のNW構成 2/2

- NWはIPv4/v6 dual stack
  - DMZはIPv4/v6 dual stack
    - DNSサーバは、IPv4/v6 dual stack
    - Mailゲートウェイは、IPv4/v6 dual stack
    - WWWサーバは，IPv4/v6 dual stack
  - 共有サーバ(SV)NWは IPv4/v6
    - 共有DNSサーバは、IPv4/v6 dual stack
    - 共有Mailサーバは、IPv4/v6 dual stack
  - Client NWはIPv4/v6 dual stack
    - DNSサーバは、IPv4
    - Mailサーバは、IPv4
- 端末PCはIPv6研究用端末のみIPv4/v6 dual stack，その他一般端末はIPv4

KDDI R&D LABS

IPv6 専用網移行における考え方 1/2

- IPv6専用化対象端末
  - 原則，日常業務に使っている全ての端末をIPv6専用化する
  - どうしてもIPv6化できない端末はIPv4専用網に収容する
  - 対象OSはWindowsXP
- 対象アプリケーション
  - Web・Mail・FTPだけを業務利用アプリケーションとする
  - Client NW外とのLPRによる印刷
  - Client NW外とのWindowsファイル共有は利用しない

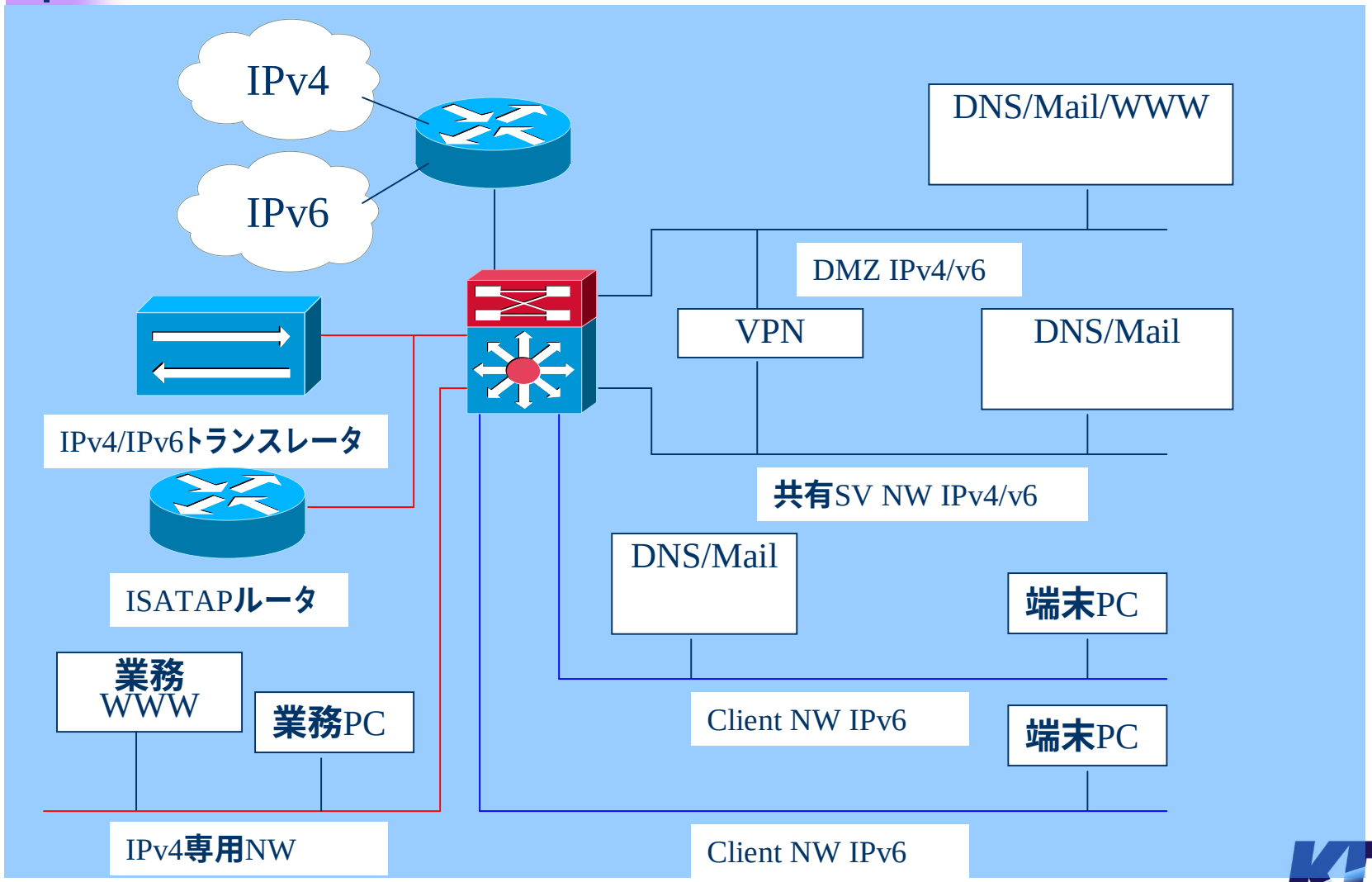
KDDI R&D LABS

IPv6 専用網移行における考え方 2/2

- ルーティング
  - Client NWへのIPv4フォワーディングを止める
  - Client NW内に閉じたIPv4通信は許可する
  - IPv4専用網を設け，NATPT IPv4/v6トランスレータ経由で相互通信させる
- 設備費･経費
  - 新規投資設備を極力避け，安価な構築を目指す
  - 社員の日常業務を妨げないため，ケーブルの新規配線は避ける

KDDI R&D LABS

IPv6 専用網移行後のNW構成 1/2



KDDI R&D LABS

IPv6 専用網移行後のNW構成 2/2

- NWはIPv4/v6 dual stack
  - DMZはIPv4/v6 dual stack
    - DNSサーバは、IPv4/v6 dual stack
    - Mailゲートウェイは、IPv4/v6 dual stack
    - WWWサーバは，IPv4/v6 dual stack
  - IPv4専用ネットワークを新設
  - 共有サーバ(SV)NWは IPv4/v6
    - 共有DNSサーバは、IPv4/v6 dual stack
    - 共有Mailサーバは、IPv4/v6 dual stack
    - NATPT　IPv4/v6トランスレータの新設
    - VPN用ISATAPルータの新設
  - Client NWはIPv6
    - DNSサーバは、IPv6
    - Mailサーバは、IPv6
- 端末PCはIPv6

KDDI R&D LABS

問題点と解決方法　サーバ編　1/3

- MTAのＳＰＡＭチェック処理の問題

  sendmailで、check_mailが設定されている環境で、ホスト名にAAAAレコードを設定しているが、Aレコードが無いサーバからの受信を拒否する。From:のチェックで引っかかる

  - 解決方法：　仮のIPv4アドレスをAレコードを追加し対応した。

- IPv4 WWWサーバ検索の問題

  DNS問題による、見えないWebサーバがある。（DNS サーバFail・AAAA無応答）

  - 解決方法：　AAAAクエリーによるDNS サーバFail無視するようにトラスレータ変更した。AAAA無応答サーバについては、タイマーによるエラー監視

  NATPTのエントリータイムアウトにより，フォーム入力ができなくなる。

  - 解決方法：　static translateを設定し、パーマネントにテーブルを作成

KDDI R&D LABS

問題点と解決方法　サーバ編　2/3

- WWWサーバ　リンクアドレスIPv4直書の問題

  <img src="http://64.4.55.45/spacer.gif" height=1 width=115>

  IPv4アドレスが直書きされている。
  - 解決方法：　サーバにでFQDNで記述する。

    Web proxyサーバを利用する。
- CISCO VPNとISATAP

  VPNにCiscoVPNを利用し、ISATAP利用する場合MTU不整合により接続できない
  - 解決方法：MTU1280になるようRAを設定

  スプリットDNSにおける、AAAAのクエリー無応答による、Web回覧の遅延
  - 解決方法：Ciscoの対応待ち
- DNSサーバのIPv4対応の問題

  DNSサーバはIPv4からのクエリに答える必要がある
  - 解決方法：Dual Stack NW上に設置

KDDI R&D LABS

問題点と解決方法　サーバ編　3/3

- .ip6.netでの逆引きの遅延

  逆引きの方法にRFC1886ニブル・フォーマットとRFC2874ビットストリング・ラベル提案されており、実装により、逆引きができない場合はある。ニブル・フォーマットが主流であるが、Linuxなどリゾルバが、ビットストリング・ラベルで問い合わせる場合がある。

  - 解決方法：サーバで、resolve.confのDNSサーバを設定しない。
    BIND9.3を導入する。

KDDI R&D LABS

問題点と解決方法　端末編 1/4

- WindowsXPのDNSクエリがIPv6に対応していない
  - 解決方法：NameServerProxyを利用
- WindowsXPのRAの問題
  - 2個以上の有効なインタフェースがあり片方がインターネットの共有があると、RAを吐きネットワークに障害を与える
  - 解決方法：XPでのインターネットの共有をしないように設定する
- WindowsXP　SP2の問題

  Windowsの立ち上げ時IPv6アドレス取得に3分～5分掛かる。RSを出してRAを受信するもアドレス付与されず。ファイアウォール設定を無効にしても同様。
  - 解決方法：MicoroSoftの対応待ちであるが、インタフェースを無効/有効にするか。ipv6 renewコマンドを入力する。
- Windowsファイル共有の問題

  セキュリティ上の問題はあるが，現実問題として Windowsファイル共有(IPv4)ができないと仕事の連係に問題が多い。
  - 解決方法：WebDAV等で代替案を提示したが，利用されていない

KDDI R&D LABS

問題点と解決方法　端末編 2/4

- **Mail ClientがIPv6のLADPに未対応の問題**

  IPv6対応メールクライアントでIPv6のLDAPに対応している物がない。

  - 解決方法：IPv6対応メールクライアントで対応まで待つ

- **Mail Clientの移行時の作業負荷の問題**

  IPv4しか使えないEudora等からIPv6対応のMozilla等へメールクライアントを変更する必要があり、利便性での苦情がある。またデータ移行時に添付ファイルを移行できない問題があった。

  - 解決方法：IPv4しか使えないメーラのIPv6化を待つ

- **無線LAN内蔵端末でIPv6アドレス未付与問題**

  Intel® Centrino™ mobile technology の端末で一部無線LANインタフェースにIPv6を付与されない

  Let'sNote　CF-W2 DW6AXS

  - 解決方法：ipv6 renewを入力する。

KDDI R&D LABS

問題点と解決方法　端末編 3/4

- **ウイルス対策ソフト**

  IPv6未対応のため、メール受信時は、チェックを行えず、メールクライアントが、受信ファイル作成した段階でウイルスを発見する。

  パターンファイルのアップデートは、ウイルス対策ソフトがIEの通信コンポーネントを使用している場合可能である。

  - 解決方法：IPv6対応ウイルス対策ソフトを待つ
  - IPv6環境下によるUPDATEを確認したソフト
    - Notron Antivirus
  - IPv6環境下によるUPDATEを確認できなかったソフト
    - McAfee VirusScan と Trend Micro ウイルスバスター

  メール受信じにウィルスチェックできないため、ウイルスメールを受信すると、メールボックスがなくなる。

  - 解決方法：IPv6対応ウイルス対策ソフトを待つ
  - Mail gateway サーバで、ウイルスチェックを強化する。

KDDI R&D LABS

問題点と解決方法　端末編 4/4

- JAVA applet

  Webブラウザが IPv6に対応していてもJAVA appletがIPv6未対応であるとJAVAアプリケーションを使用できない。

  - 解決方法：JAVA appletをIPv6対応とする
- Mozillaでバナー広告が、接続タイムアウトする

  ad.jp.doubleclick.netのバナーを表示しようとしてエラーとなる。

  IEでは、正常に表示する。

  - 解決方法：proxyを利用する
- どうしてもIPv4アプリを使いたい場合

  メールクライアントを変更したくない場合・LDAPを使いたい場合

  - 解決方法：WindowsXP標準のportproxyを利用する。

    sshを利用しPortForwardする。

KDDI R&D LABS

移行して分かった事

- DNS

  サーバが、AAAAのクエリーに対して、DNS サーバFail・無応答であるため、アドレス解決に時間がかかかるか、サーバに接続できない。

  ・Cisco VPN・Webサーバ

- IPv6対応アプリでも、オプション機能が、IPv6対応になっていない

  ・MailクライアントのLDAP検索

- Windows系では、IPv4アドレスはどうしても必要

  ・DNSクエリーのトランスポートがIPv4であるため。

KDDI R&D LABS

その他

- IPv6化に使用した機材
  - IPv4/IPv6トランスレータ　日立製作所　AG8100S-T
  - ISATAPルータ　Cisco　7200　(IOS12.3(8)T3)
  - 基幹ルータSW　Foundry　BigIron8000
  - プリントサーバ　silex　PRICOM 3100
- ネットワーク工事

  VLANおよび情報コンセントを使用し配線工事を極力少なくした。
- DNSへの自動登録

  RAによる、IPv6アドレスの生成では、端末アドレスのDNSへの登録は難しいので、DNS登録ツールの開発を予定している。
- IPv6対応テレビ会議システム

  トランスレータを経由した、IPv4-IPv6相互通信によるテレビ会議システム(QM) の接続確認を実施した。

  QM – QualityMeeting KDDI研究所が開発したテレビ会議システム

KDDI R&D LABS