覚えて帰ろうIPv6最新情報

～標準化動向から設定ノウハウまで～

【IPv6ネットワーク設定TIPS編】

2006年12月5日

＜改訂版＞

IPv6普及・高度化推進協議会 IPv6対応OS評価SWG
株式会社インテック・ネットコア IPv6研究開発グループ
北口　善明
kitaguchi@inetcore.com

IPv6ネットワーク設定TIPS編　目次

背景

- Windows Vistaの登場
  - 代表的なコンシューマOSがIPv6に完全対応
    - GUIによるIPv6設定
    - IPv4/IPv6を意識させないAPI
  - ほとんどのWindowsコンポーネントがIPv6対応に
  - IPv6 onlyは容易（IPv4 onlyは基本的に不可）
    - IPv4だけ知っていれば良い環境ではなくなりつつある
- IPv6普及・高度化推進協議会における取り組み
  - IPv6対応OS評価SWGにて端末のIPv6対応における影響を議論
    - http://www.v6pc.jp/jp/wg/transWG/osSWG.phtml
  - ガイドラインの作成（2007年1月31日に第1版を公開予定）
    - “IPv6端末OSにおけるIPv6対応・IPv6機能活用ガイドライン”

DNS関連の注意点

DNS

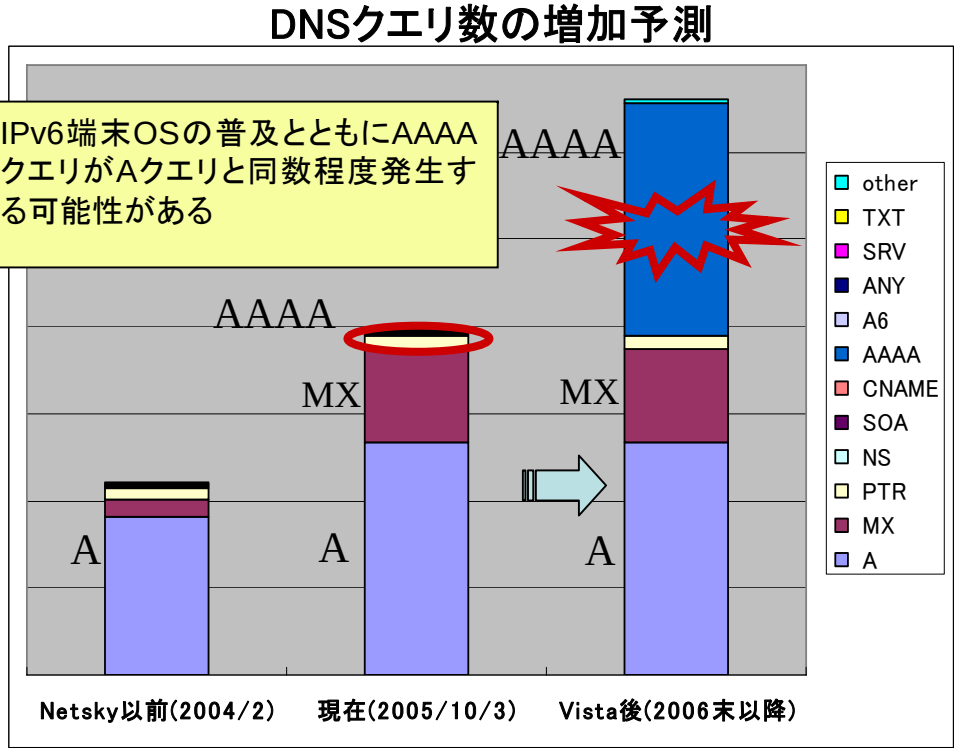
DNSクエリ増加

- デュアルスタックによるDNSクエリの倍増
  - Aレコード解決＋AAAAレコード解決＝約２倍
- DNSサフィックス付加機能
  - OSにより付加（DHCPで配られるドメイン名等）
  - 検索エンジンにより付加（Webブラウザの機能）
- 具体例

ドメインサフィックスに「.co.jp」と「.example.jp」がある時の“ns”名前解決

A	ns
A	ns.co.jp
A	ns.example.jp
AAAA	ns
AAAA	ns.co.jp
AAAA	ns.example.jp

最大6つのクエリが発生



「IPv6端末OSにおけるIPv6対応・IPv6機能活用ガイドライン」より

DNS不正応答問題

DNS iNetCore

- AAAAレコード解決への対応不備（RFC4074）
  - ５つの代表的な不正応答が存在

> ① AAAAレコードの問い合わせを無視
> ② NXDOMAIN（RCODE=3）を返す
> ③ NXDOMAIN以外の不正なRCODEを返す
> ④ 壊れた返答/IPv4アドレスを返す
> ⑤ Lame Delegationになる
> ※正しい応答はNOERROR（RCODE=0）で中身が空

  - ロードバランサ、ファイアウォール、ホテルインターネットなどの機器で上記の不具合を引き起こすものがある
- 具体的な不具合：キャプティブ・ポータル問題
  - 複数の問題が原因で発生した（Windows XP SP2 + IPv6）
    - OSはIPv6の到達性がないのにAAAAレコード解決を行う
    - 未対応機器はAAAAレコード解決にIPv4アドレスを返す
    - OSは壊れた応答にも関らず受理するため処理が失敗に

DNSクエリに関するOSの対応

DNS iNetCore

- DNSリゾルバの改良
  - Aレコード解決を優先する（FreeBSD、Windows Vista）
    - IPv6が優勢になった時に問題になる可能性あり
  - Aレコード解決時にNXDOMAINならAAAAレコード解決をしない（Windows Vista）
  - Aレコードのレスポンス時間によりAAAAレコードの処理待ち時間を決定（FreeBSD、Windows Vista）
    - AAAAレコードがない場合のタイムアウト時間を小さくするため
- AAAAレコード解決の抑制
  - グローバルIPv6アドレス※が付与されない限りAAAAクエリによる名前解決は実施しない（Windows Vista）

    ※ 6to4およびTeredoアドレスを除くグローバルIPv6アドレス

DNSクエリの順序

- クエリ順序はOSで異なる
  - FreeBSD-5.5R
    - IPv4の名前解決とIPv6の名前解決を交互に繰り返し名前解決ができた時点で終了
  - Windows XP SP2
    - まずIPv6の名前解決を全て実施し次にIPv4の名前解決を全て実施
  - Windows Vista
    - まずIPv4の名前解決を全て実施し次にNXDOMAINが返されたもの以外の全てに関してIPv6の名前解決を実施
- 先ほどの具体例におけるOS毎の挙動

FreeBSD-5.5R

A	ns
AAAA	ns
A	ns.co.jp
AAAA	ns.co.jp
A	ns.example.jp
AAAA	ns.example.jp

Windows XP SP2

AAAA	ns
AAAA	ns.co.jp
AAAA	ns.example.jp
A	ns
A	ns.co.jp
A	ns.example.jp

Windows Vista

A	ns
A	ns.co.jp
A	ns.example.jp
AAAA	ns.example.jp

製品版反映箇所

※ ns.とns.co.jp.がNXXOMAINの場合の挙動例

IPv6とDNS設定

DNS iNetCore

- DNSディスカバリ
  - DNSサーバアドレス取得方法に３種類の提案（RFC4339）
    - RAによる通知（RDNSSオプション）　検討中
    - DHCPv6による通知　実装あり
    - Well-known Anycast Addressの利用　サイトローカル利用に問題
  - DHCPv6による設定が一般的
    - RAの“Managed-Flag = 1”で端末はDHCPv6による設定を実行
- ダイナミックDNS
  - IPv6におけるDNSサーバ運用負荷の増大
    - アドレス数の増加、アドレス長が長い
  - 運用負荷軽減のためIPv6では期待大

セキュリティ関連の注意点

Security

自動トンネルの認識

- IPv4ネットワーク上にIPv6到達性を実現
  - 管理者、利用者の正しい把握が必要
  - IPv4しかなくてもIPv6が利用されている認識が必要
- 6to4（RFC3056）
  - IPv4アドレスを基に生成されるIPv6プレフィックス
  - 6to4ゲートウェイを介してIPv6ネットワークへ接続
- Teredo（RFC4380）
  - IPv4のUDP（3544）を利用するトンネリング技術
  - Teredoサーバを介したNAT越えによるIPv6ネットワークへの接続
- Windows Vistaでの挙動は？
  - グローバルIPv4アドレス環境下で6to4インタフェースが自動生成
    - （例）219.118.97.6を持つ端末は2002:db76:6106::/48が利用可能

      ※ ただしRAによるIPv6アドレスが付与されると利用されない
  - NAT配下の環境にてTeredoインタフェースが自動生成
    - IPv6アドレスが1つだけ利用可能

      ※ ただしRAによるIPv6アドレスが付与されると利用されない

IPv6におけるパケットフィルタ Security

- IPv6ネットワークではパケットフィルタは重要
  - パケットフィルタの設定はIPv4と変わらない
  - 基本的にEnd-to-endの通信なので端末でしっかり守る
- IPv6ネットワークでの注意点
  - ICMPv6パケットは止めない
    - MTUディスカバリなどIPv6ネットワークでは重要
  - EDNS0やTCP53も通す
    - IPv6ではDNS回答パケットが大きくなりがちなためほぼ必須
- 拡張ヘッダへの対応
  - 単純なパケットフィルタでは対応できないものもある
    - ルーティングヘッダ、フラグメントヘッダ等
  - ファイアウォール製品の利用も検討が必要

意図しない/不正なRAへの対応

Security

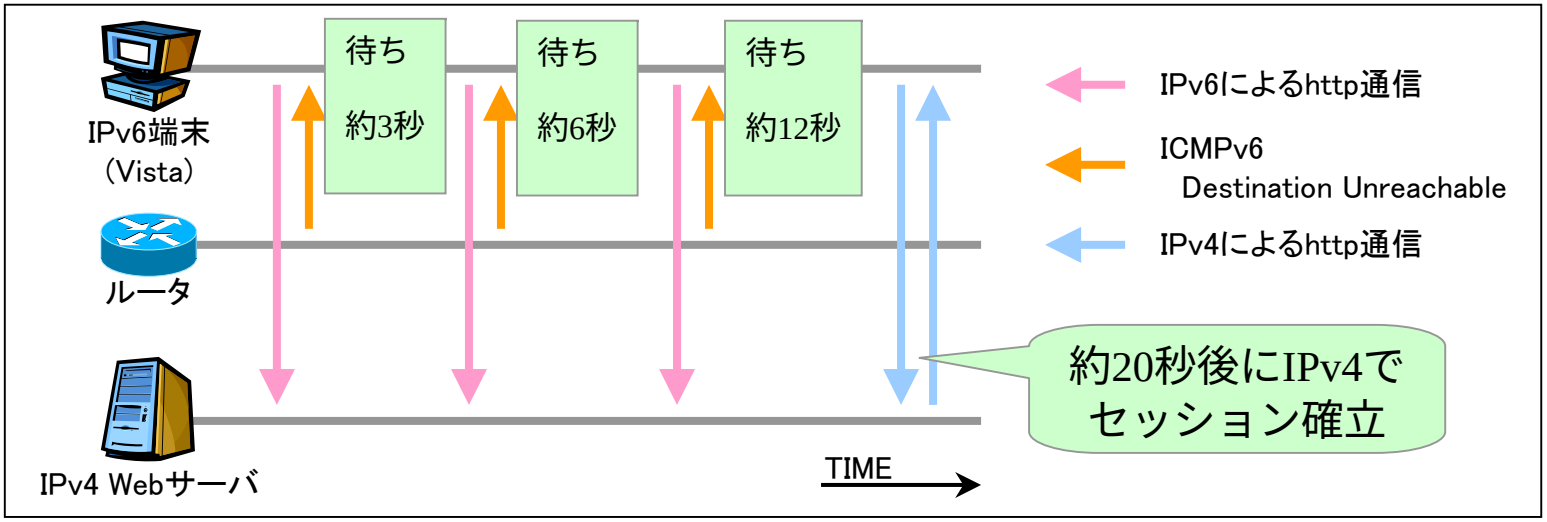
- RA（ルータ広告）受信によりIPv6対応端末は通信可能に
  - IPv4のみのセグメントでもIPv6アドレスが付加
  - 悪意のあるRAによるパケット収集の危険
    - 誰でもデフォルトルートになれる事が問題
- 対策方法
  - SEND（RFC3971）の利用
    - 権利上の問題等で普及に至ってない
  - スイッチによる制御
    - ルータを接続するポートからのみRAを許可する
    - ICMPv6　Type=134 （対応スイッチが必要）
  - 端末による制御
    - RAをパーソナルファイアウォールなどで制限
      - RS（ルータ要請）も停止する必要あり
    - IPv6無効化は最終手段．．．

デュアルスタック関連の注意点 Dualstack

IPv6閉域ネットワーク問題

Dualstack iNetCore

- グローバルな到達性がないと
  - IPv6アドレスへの通信をとりあえず試みるため問題
  - IPv4ネットワークへの接続に時間がかかる
- TCPフォールバック問題
  - ICMPv6によるDestination Unreachableが返っても
    - 端末OSでの挙動は規定がないためフォールバックする実装は少ない
  - Windows Vistaでは
    - 3回通信を試みた後IPv4での接続に移行
    - 20秒くらい接続まで時間がかかることに



TCPフォールバック問題対策 Dualstack

- デフォルトルートの削除
  - RAでデフォルトルートを設定しない
  - IPv6閉域ネットワークプレフィックスの経路のみ設定
  - RFC4191による経路配布の利用が適切
- アドレス選択機構による制御（RFC3484）
  - 送信元アドレス選択順序をポリシテーブルにて定義
  - IPv4アドレス（::ffff:0:0/96）の優先度を高くする
- OS側の実装による対応
  - ICMPv6のDestination Unreachable受信時の挙動変更
  - コネクション確立時に限り素早くフォールバックする手法
  - draft-ietf-tcpm-tcp-soft-errors-02.txt

ネットワーク運用での注意点 Operation

アドレス設計

- グローバルアドレスの利用
  - アドレス取得が不可な場合ULAの利用も可能
  - 集約可能なアドレス設計が重要
- 全てのサブネットに/64
  - PtoPセグメントも/64で問題なし
- サーバには固定アドレス
  - 管理者が記憶しやすいものが良い
    - ＜プレフィックス＞::＜ポート番号＞:＜連番＞など
    - （例）2001:200:562::80:1　　Webサーバ
- IPv4射影IPv6アドレスに関して
  - IPv4アドレスをIPv6アドレスとして扱うアドレス
    - （例）::ffff:192.168.0.1/96
  - サーバ運用上問題の種となるためサーバでは無効化が無難

ルーティングプロトコル

- IPv4とIPv6の経路制御は独立させる
  - マルチプロトコル対応の場合でも分離
- ルーティングプロトコルの種類

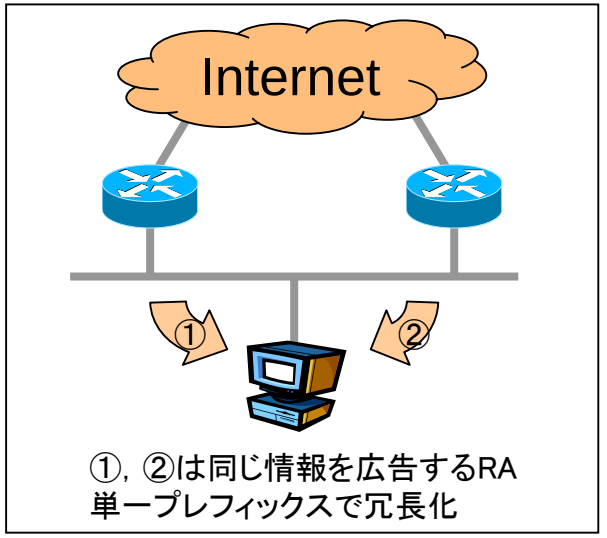
Type	IPv4	IPv6
IGP	RIPv2	RIPng
	OSPFv2	OSPFv3
	ISIS	ISIS
EGP	BGP4	BGP4+
Multicast	PIM	PIM

- ルーティングプロトコルの選択
  - IGPではスタティックが有効
  - OSPFv3も安定しているため規模により選択
  - ルータによりASを分けて取り扱えないためBGPでは注意が必要

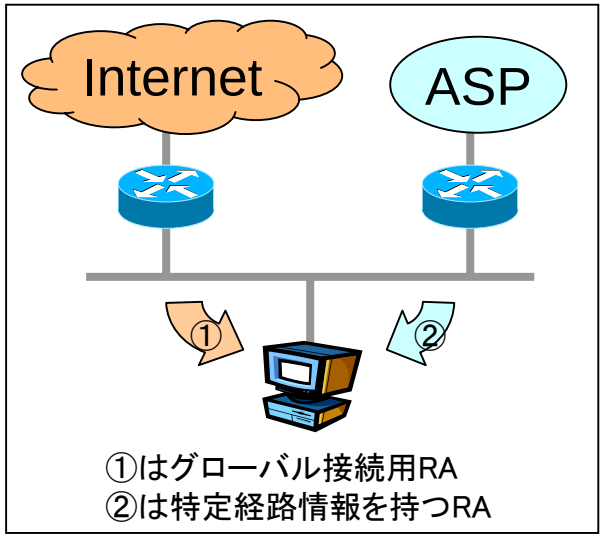
マルチホーミング

- RAをVRRPv6の代用とする利用
  - Lifetimeや広告間隔を短くすることで可能
  - 経路の冗長化のための単純なマルチホーム
- RFC4191の可能性
  - ルータ優先度指定
    - 明示的なバックアップルータの指定が可能
  - 特定経路広告が可能
    - IPv6閉域ネットワークとの連携が可能
    - RFC3484のアドレス選択機構が必須
- 高度なマルチホーミング
  - shim6
    - エンドノードによるトラフィック制御
  - IPv6 PIアドレス
    - BGP利用のマルチホーミング

経路冗長マルチホーム



マルチプレフィックス



IPv6ネットワーク設定の具体例

TIPS

ネットワーク設定

TIPS iNetCore

- RAの設定
  - ルータ機器では基本的にインタフェースのIPv6対応で設定
    - 停止する場合には明示的な設定が必要
  - 端末OSでは複数のインタフェースが有効でRAが送信されるものもあるため注意が必要
- 経路制御（BGP4+とOSPFv3利用の設定例）

Cisco Router Config

```
ipv6 unicast-routing
ipv6 cef
!
interface FastEthernet1/0
 ip address 210.248.164.229 255.255.255.248
 ipv6 enable
 ipv6 address 2001:218:1:1045::229/64
 ipv6 ospf 3949 area 0
!
interface FastEthernet1/1
 ip address 210.163.36.9 255.255.255.248
 ipv6 enable
 ipv6 address 2001:218:1f01:f010::1/64
!
router ospf 65037
 network 210.163.36.8 0.0.0.7 area 0
 network 210.348.164.224 0.0.0.7 area 0
```

```
!
router bgp 3949
 bgp log-neighbor-changes
 neighbor 2001:218:1:1045::1 remote-as 3949
 address family ipv4
 no neighbor 2001:218:1:1045::1 active
 exit-address-family
 !
 address-family ipv6
 neighbor 2001:218:1:1045::1 active
 exit-address-family
!
ip classless
!
ipv6 route ::/0 2001:218:1f01:f000::/56 Null0
ipv6 router ospf 3949
 redistribute static
access-list 99 permit 210.163.36.8 0.0.0.7
!
```

```
ipv6 access-list acl99
 permit ipv6 2001:218:1f01:f010::/64 any
 permit ipv6 host 2001:218:1:1040::4 any
 deny ipv6 any any
!
line vty 0 4
 access-class 99 in
 ipv6 access-class acl99 in
```

各種サーバの設定（１）

TIPS iNetCore

- サーバのIPアドレス設定
  - インタフェースIDの手動設定も可能
    - ifconfig fxp0 inet6 fe80::10
  - RA受信によるグローバルアドレスにも反映される
    - fe80::10 + RA（2001:200:562::/64）⇒ 2001:200:562::10/64
- DNSサーバ
  - bind-9.3以降の利用が無難
  - 正引きはAAAAレコード、逆引きは.ip6.arpaのみ設定
  - MXレコードのIPv6対応はサーバの対応も必ず実施
  - AAAAレコード回答に対応しているか確認する
    - **http://www.cnri.dit.ie/cgi-bin/check_aaaa.pl**　にて回答を確認可能
      ※IPv4のみのDNSサーバも確認するべし
- メールサーバ
  - Postfix、SendmailなどIPv6対応済み
    - postfix/main.cf：”inet_protocols=all”
    - sendmail.cf：”O DaemonPortOptions=Name=IPv6, Family=inet6”

各種サーバの設定（２）

TIPS iNetCore

- Webサーバ
  - Apache2、IIS6.0などがIPv6対応済み
  - バーチャルホストでプロトコル毎に異なるページ設定も可能

httpd.conf

```
<VirtualHost 192.168.0.80:80>
 DocumentRoot /usr/local/www/htdocs
 …
</VirtualHost>
<VirtualHost [2001:200:562::80:1]:80>
 DocumentRoot /usr/local/www/htdocs_v6
 …
</VirturalHost>
```

- アプリケーションサーバのIPv6化
  - ほとんどのアプリケーションはIPv6対応している
  - SSHポートフォワーディングの利用も便利
  - Windowsのport proxyも有効

IPv4通信優先設定

TIPS iNetCore

- IPv4通信を先に試みる設定（IPv6無効とは異なる）
  - ポリシテーブルの設定で“::ffff:0:0/96”を最優先に
  - getaddrinfoの戻り値がポリシの順にソートされる

Windows XP SP2 の場合

```
> netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0
> netsh interface ipv6 set prefixpolicy ::1/128 40 1
> netsh interface ipv6 set prefixpolicy ::/0 30 2
> netsh interface ipv6 set prefixpolicy 2002::/16 20 3
> netsh interface ipv6 set prefixpolicy ::/96 10 4
> netsh interface ipv6 set prefixpolicy 3ffe:831f::/32 5 5
```

Windows Vista の場合

```
> netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0
> netsh interface ipv6 add prefixpolicy ::1/128 40 1
> netsh interface ipv6 add prefixpolicy ::/0 30 2
> netsh interface ipv6 add prefixpolicy 2002::/16 20 3
> netsh interface ipv6 add prefixpolicy ::/96 10 4
> netsh interface ipv6 add prefixpolicy 3ffe:831f::/32 5 5
```

設定の確認コマンド（Windows 共通）

```
> netsh interface ipv6 show prefixpolicy
```

FreeBSD 5.5R の場合

```
# ip6addrctl flush
# ip6addrctl add ::ffff:0:0/96 50 0
# ip6addrctl add ::1/128 40 1
# ip6addrctl add ::/0 30 2
# ip6addrctl add 2002::/16 20 3
# ip6addrctl add ::/96 10 4
```

設定スクリプトの利用

```
# /etc/rc.d/ip6addrctl prefer_ipv4
```

※/etc/rc.confに「ipv6addrctl_enable=“YES”」が必要

設定の確認コマンド

```
# ip6addrctl show
```

RA受信拒否設定

TIPS iNetCore

- IPv6対応機器に自動的にアドレス設定させない設定
  - IPv6が普及してもIPv4 onlyセグメントは残る場合
  - IPv6アドレスやデフォルト経路設定を手動で実施する場合

FreeBSD 5.5R の場合
（NetBSD、Mac OS X も同様）

```
# sysctl –w net.inet6.ip6.accept_rtadv=0
```

Windows XP SP2 の場合

※RA受信拒否設定は存在しないために拒否したい
インタフェースのプロトコル設定から
「Microsoft TCP/IP version6」を削除する

Linux の場合

```
# echo 0 > /proc/sys/net/ipv6/conf/all/accept_ra
# echo 0 > /proc/sys/net/ipv6/conf/eth0/autoconf
```

※/etc/sysconfig/network-scripts/ifcfg-<iface>に
「IPV6_AUTOCONF="no"」の設定も可（Redhat系）

Windows Vista の場合

```
> netsh interface ipv6 set interface "<ID>"
                              routerdiscovery=disabled
```

※<ID>にはインタフェースIDを指定
インタフェースIDはリンクローカルアドレスの%以下
で確認することができる
例） fe80::230:48ff:fe74:9779%8
またdisabledをdhcpとするとDHCPv6の利用となる

製品版反映箇所

まとめ

- IPv6対応は確実に進んでいる
  - 知らないうちに機器がIPv6対応になっている
  - IPv6ネットワークサービスも容易に手に入る
  - IPv6に無関心のままではまずい
- デュアルスタックネットワークは容易に構築可能
  - デュアルスタック時の注意点の把握は必要
  - IPv4しか使わないネットワークでの対策は重要
- IPv6普及の起爆剤としてのWindows Vista
  - Windows Vista上の開発アプリケーションはIPv6対応になる
  - IPv6の特徴を用いたアプリケーションに期待
    - アドホックネットワークとIPv6
    - P2PアプリケーションとIPv6

参考資料

- IPv6普及・高度化推進協議会
  - http://www.v6pc.jp/
- IPv6 FORUM
  - http://www.ipv6forum.com/
- IETF
  - http://www.ietf.org/
- IPv6 to Standard
  - http://www.ipv6-to-standard.org/
- IPv6 Style!
  - http://www.ipv6style.jp/
- IPv6 Portal
  - http://www.ipv6tf.org/
- ビジネス on IPv6
  - http://www.biz6.jp/