デュアルスタックの苦悩:サーバ編
JANOG23 高知

(株)クララオンライン
白畑　真 <shin@clara.ad.jp>

クライアントだけじゃなくて
サーバも対応しなきゃ

ホスティング事業者として

「IPv6でどんと来い！」

…と言えるように

- お客様がIPv4でアクセスされる場合もIPv6でアクセスされる場合も、同様にサービスを提供する手法を検討
- 検討事項
  - 新規サービスのIPv6対応
  - 既存サービスのIPv6対応

ご注意:

- 2009年1月現在、(株)クララオンラインはIPv6対応のサービスの提供は行っておりません。
- 本発表はIPv4/IP6 デュアルスタックサービスの展開手法についての一検討であり、特定のプロダクトまたはサービスを推奨するものではありません。

第1回・第2回実証実験にて

- 最近のOSでは、パッチをあてなくても標準のソフトウェアでIPv6が動く
  - IPv6ネットワークさえあればいける!?

- めでたしめでたし

....と思いきや、いくつか地雷が...

ソフトウェアの設定の違い

- IPv6対応状況の違い
  - デフォルト設定のIPv6対応状況が異なる

初期設定値(*1)	IPv6有効	IPv6無効
*1: RedHat Enterprise Linux 5 の標準構成の場合	Apache (Web) Dovecot (POP3) OpenSSH (SSH)	BIND (DNS) Postfix (SMTP) Sendmail (SMTP) vsftpd (FTP)

- 設定ファイルの書式の違い
  - IPv6アドレスを“[”，“]”で囲むか否か
    例: [2002:db8::]/64派 vs. 2001:db8::/64派

IPv4射影アドレス

IPv4射影アドレス(IPv4-mapped IPv6 address):
IPv4アドレスを表す特殊なIPv6アドレス
例: IPv4の“**192.0.2.1**”に相当するアドレスを“**::ffff:192.0.2.1**”として表現

- IPv6対応のアプリケーションには、IPv4の扱い方に二種類ある
  1. (IPv4シングルスタックの場合とは異なり) IPv6用ソケットで**IPv4射影アドレス**を利用
  2. (従来同様) IPv4用のソケットを利用
- OSやアプリケーションの仕様や設定によってデフォルト設定、実装がまちまち

IPv4射影アドレスの問題点

- draft-itojun-v6ops-v4mapped-harmful-02 (IPv4-Mapped Address API Considered Harmful) の指摘
  - 実装の複雑化
    - 多くのOSではIPv4射影アドレスを無効化できる
    - IPv4射影アドレスを無効化した場合、IPv6でのみ動作するようになるアプリケーションも
  - アクセス制御が複雑化
    - IPv4 射影アドレス用の設定が必要になる場合も
    - 同一のIPv4ホストとの通信でも、OSやアプリケーションによって見え方が異なる
  - コードの移植性が低下

デュアルスタックとソケットの関係

IPv4射影アドレスが無効なデュアルスタック環境では…

1. “0.0.0.0”の代わりに“::” をListenする環境では、IPv4接続をサポートしない
2. “0.0.0.0“に加えて“::” をListenする環境では、IPv4接続に関する挙動は変わらない

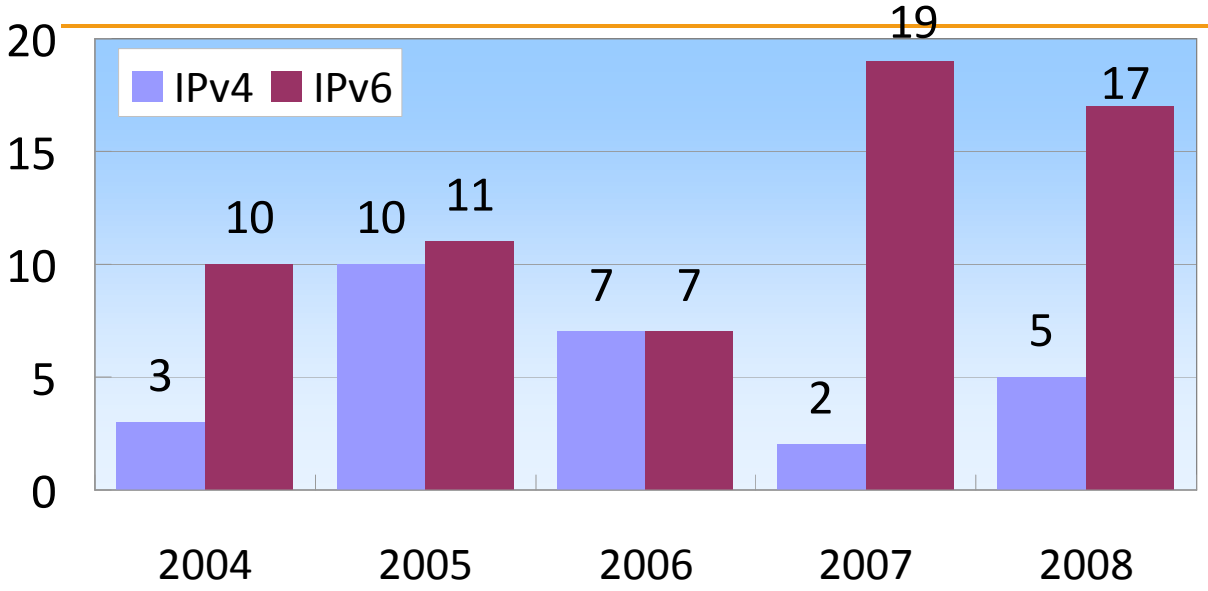
Socketの構成		IPv6クライアントからの接続	IPv4クライアントからの接続
	IPV6_V6ONLY ソケットオプション		
0.0.0.0 IN_ADDR_ANY		×	○ 192.0.2.1
:: IN6_ADDR_ANY	Yes (IPv4射影アドレスを利用しない)	○	×
	No (IPv4射影アドレスを利用する)	○	○::ffff:192.0.2.1 IPv4射影アドレス

OS Specificなネタですが…
Linux kernel 2.6の問題

- IPv6のアドレス自動構成を無効にした場合、デフォルトルートの設定が有効にならないケースがある
  - 経路が存在するのにも関わらず、**ping**すると“**connect: Network is unreachable**”
  - とりあえず0::/1の経路を追加してお茶を濁す…
- 2007年6月に修正版がkernelに反映されたものの…
  - RedHat Enterprise Linux 5.2 の kernel には修正コードは含まれていない
  - 1/21にリリースされた RedHat Enterprise Linux 5.3 で修正済み
- 詳細:
  - http://bugzilla.kernel.org/show_bug.cgi?id=8349
  - https://bugzilla.redhat.com/show_bug.cgi?id=243526

残念なお知らせ:
IPv6実装はまだ枯れていない

IPv4/IPv6 プロトコルスタック脆弱性のアドバイザリ公表件数の推移



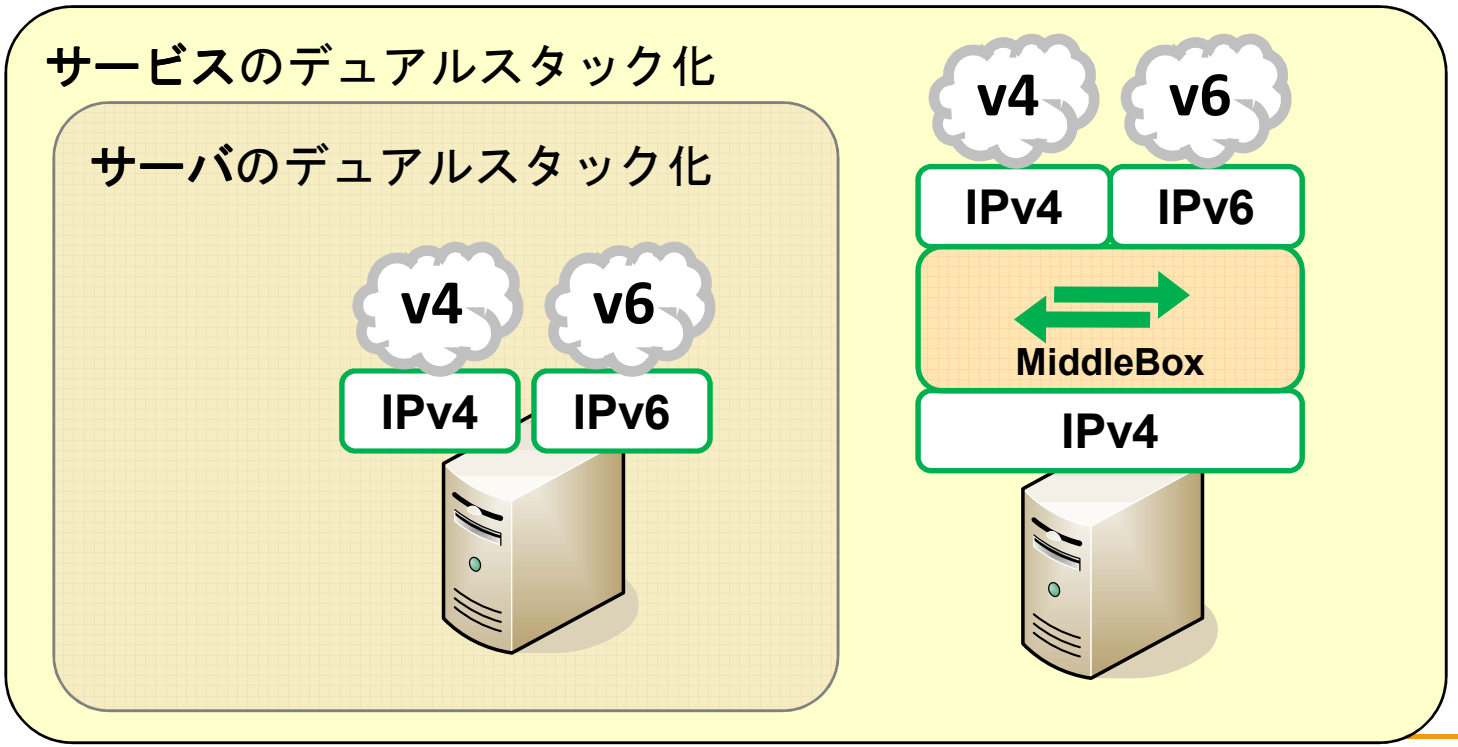
出典：Secunia 社の Secunia Advisories Database より発表者が作成

- IPv6を有効にした場合、IPv6特有の問題によりセキュリティリスクやメンテナンス回数が増加する可能性がある
- IPv6 特有のセキュリティホールの例
  - IPv6 Neighbor Discovery Protocol Neighbor Solicitation Vulnerability (CVE-2008-2476)
  - IPv6 Type 0 Routing Header Vulnerability (CVE-2007-2242)

サービス != サーバ

サービスのデュアルスタック化

- Middleboxを介したプロトコル変換
  - Middlebox: トランスレータ、ロードバランサ、リバースプロキシ、ファイヤウォール、CDN等
- **サーバはIPv4シングルスタックのままでよい**



まとめ: Get ready for IPv6

- サーバのIPv4/IPv6デュアルスタック化
  - 新しいOSは一通りIPv6には対応
  - 各OSやソフトウェアのIPv6対応手法は、個別の実装や設定により大きく異なる
    - 実装品質、IPv4射影アドレスとソケットの関係 etc..
- サービスのデュアルスタック化なら、IPv4 Onlyのサーバでもできる
  - MiddleboxによるIPv4/IPv6プロトコル変換
  - 影響範囲を局所化

これでサービス側もIPv6 ready.
iDC側は果たして!?

To be continued…