Internet Week 2009

点検！IPv6のセキュリティ ～サーバ編～

白畑　真
(株)クララオンライン

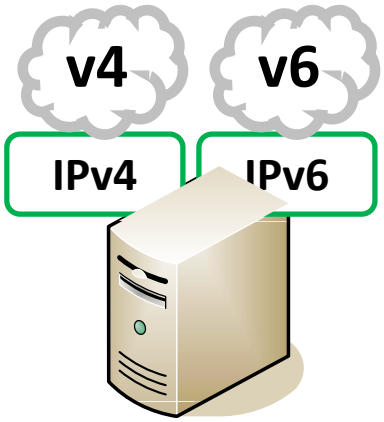
Agenda

- はじめに
- IPv6対応にあたっての課題
- サーバでのIPv4/IPv6デュアルスタック構成
- IPv4シングルスタック＋ミドルボックス構成
- IPv4/IPv6プロトコルスタックのセキュリティホールの傾向
- まとめ

はじめに

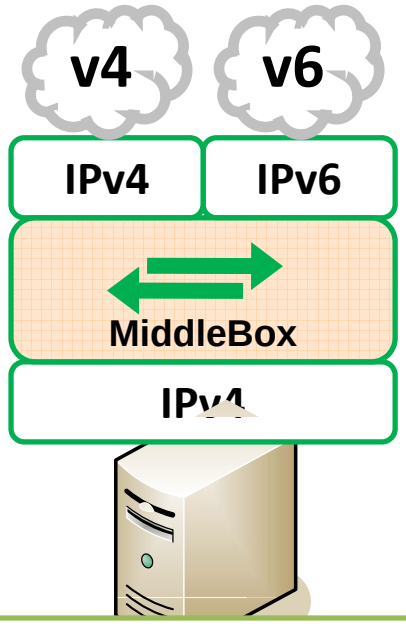
サービスにおける二つのIPv6対応手法

サーバをIPv4/IPv6デュアルスタックで運用する構成



サーバ自体はIPv4シングルスタック運用。ミドルボックスでIPv4/IPv6を変換

トランスレータ、ロードバランサ、リバースプロキシなどのミドルボックスを利用し、IPv4・IPv6を変換



前提: ネットワークはIPv4/IPv6デュアルスタック

IPv6対応にあたっての課題

IPv6シングルスタック・IPv4/IPv6デュアルスタック共通の課題

意図せず有効になるIPv6

デフォルト設定に注意

» 多くのOSではデフォルト設定でIPv6が有効
  – リンクローカルアドレスが自動的に設定されている
  – 自動トンネル(6to4, Teredoなど) – 特にクライアント向けOS

» RAの広報など、ネットワーク側がIPv6に対応したタイミングで、意図しないうちにIPv6対応になる可能性
  – Linuxサーバの場合の例:
    • IPv4ではiptablesでパケットフィルタリングされている
    • IPv6ではip6tablesでパケットフィルタリングされていない
  – **サーバ側で直接IPv6サービスを提供しないのであれば、IPv6機能の無効化を検討すべき**
    • きちんとセキュリティ対策を講じた上でIPv6の対応を

各種OSとIPv6対応

OS	IPv6対応	OSデフォルト設定のIPv6対応
Red Hat Enterprise Linux 3	○	×
Red Hat Enterprise Linux 4/5	○	○
FreeBSD 4.x	○	×
FreeBSD 8 (開発中)	○	○
Mac OS X 10.3 "Panther"	○	○
Windows Server 2003, Windows XP	○	×
Windows Server 2008, Windows Vista	○	○

簡単な確認方法
インタフェースにリンクローカルアドレス(“fe80::”で始まるアドレス)が
設定されているか

IPv6特有の課題

» Privacy Extensions (匿名アドレス/一時アドレス)

– 多くのクライアント向けOSでは、RA/DHCPv6でIPv6アドレス設定を行うとデフォルトで有効に

– IPv6アドレスを一定時間で使い捨て

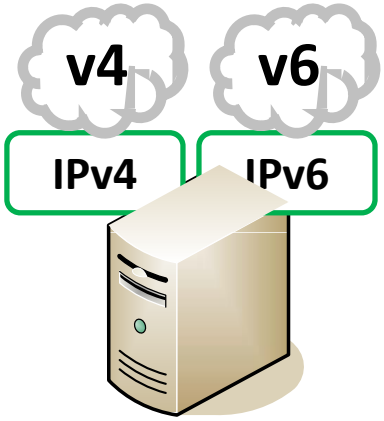
- 同一ホストのホストからのアクセスでも、時間の経過と共にIPv6アドレスが変更される
- IPv6アドレスからクライアントを特定することが困難になるため、トレードオフを検討したうえで匿名アドレスを無効化する選択も

→**サーバではIPv6アドレスを手動設定する**

IPv6特有のセキュリティホール

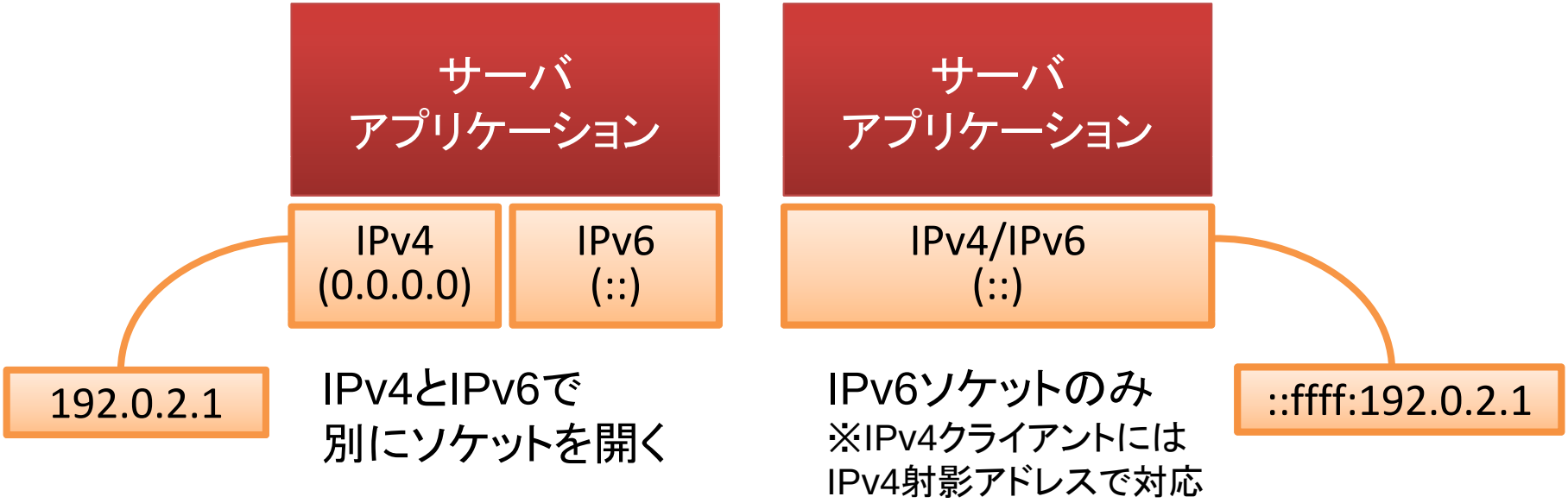
- プロトコル仕様上の欠陥
  - 例: IPv6 Type 0 Routing Header Vulnerability (CVE-2007-2242)
- プロトコル実装上の欠陥
  - 例1: IPv6 Neighbor Discovery Protocol Neighbor Solicitation Vulnerability (CVE-2008-2476)
  - 例2: IPv6 を実装した複数の製品にサービス運用妨害 (DoS) の脆弱性 (JVN#75368899)
    - 大量のIPv6アドレスやNDPエントリを生成させるDoS攻撃
- プロトコルスタックの成熟度
  - 歴史的には、IPv4プロトコルスタックに重大なセキュリティホールが発見されてきた
  - 例: 1996年の Ping of Death攻撃, 2004年のPath MTU Discovery攻撃

サーバでのIPv4/IPv6デュアルスタック



IPv6対応サーバアプリケーションとソケットの実装方法

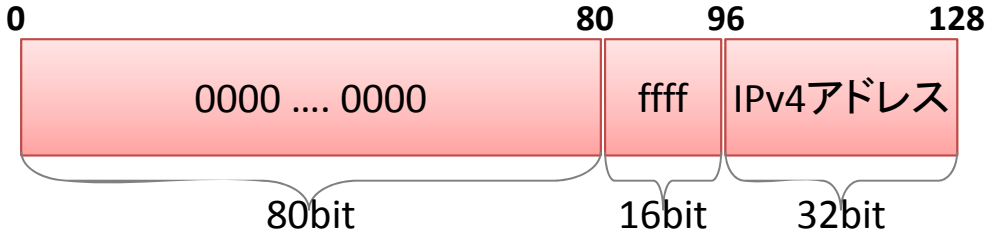
» アプリケーションのIPv4/IPv6デュアルスタック対応方式には2種類の方法がある
  – OSやアプリケーションの実装、設定により異なる
  – ログ取得やアクセス制御に互換性がない場合も



どちらの実装になっているかを把握することが重要

IPv4射影アドレス(IPv4 Mapped Address)とは

» IPv4アドレスをIPv6アドレスとして表す特殊なIPv6アドレス



» 例: 192.0.2.128 の場合

::ffff:192.0.2.128 もしくは ::ffff:c000:280

» IPv6対応アプリケーションが、IPv4/IPv6対応のソケット(“::”)で IPv4のみを持つノードと通信する際に利用

– ノード内部での利用に限定
– 送信元・宛先アドレスとしては利用されない

例: OpenSSHの場合

■ IPv4/IPv6で別々にソケットをbind(2)する場合

“netstat –an”コマンドの結果:

```
tcp    0 0 0.0.0.0:22          0.0.0.0:*          LISTEN
tcp    0 0 :::22               :::*               LISTEN
```

sshd_configファイルの設定:
ListenAddress 0.0.0.0
ListenAddress ::

■ IPv6のみでソケットをbind(2)する場合

“netstat –an”コマンドの結果:

```
tcp    0 0 :::22               :::*               LISTEN
```

sshd_configファイルの設定:
ListenAddress ::

アプリケーションによっては、設定ファイルや
コマンドラインでソケットの構成方法を変更できる場合もある

各種OSとIPv4射影アドレス

OS	IPv4射影アドレスの対応	OS全体での無効方法化
Linux 2.6	デフォルト状態で有効	net.ipv6.bindv6only変数を1に変更
FreeBSD 5.x 以降	デフォルト状態で無効	
Mac OS X	デフォルト状態で有効	net.inet6.ip6.v6only変数を1に変更
Windows Server 2003, Windows XP 以前	無効	なし
Windows Server 2008, Windows Vista 以降	有効	なし

サーバアプリケーション側の対応:
ソースコードを、IPV6_V6ONLY ソケットオプションを設定するように
改修することで無効化可能

IPv4 射影アドレスを利用しない環境では、IPv4クライアントからの接続を
受け付けるために**IPv6のソケットとは別に**IPv4のソケットを開く必要がある

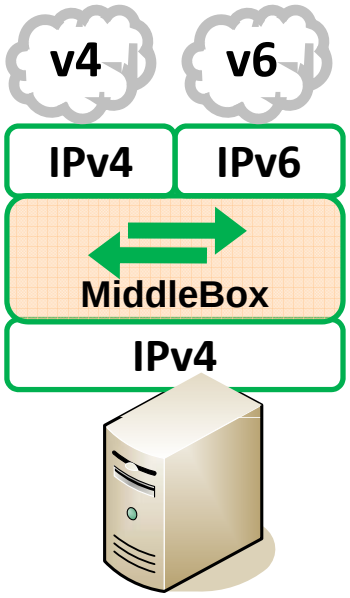
IPv4射影アドレスの問題点

» 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

IPv4/IPv6デュアルスタック環境特有のセキュリティホール

- CVE-2008-1153
  - ネットワーク機器に対して特殊なIPv6パケットを送ることで、当該機器のIPv4のサービスに対してDoS攻撃が成立する脆弱性
- CVE-2006-6263, CVE-2006-6266, CVE-2007-3038
  - IPv4/IPv6共存技術であるTeredoクライアントを踏み台として悪用する攻撃
- CVE-2007-1338
  - CPEのIPv6トンネルの設定不備に関する脆弱性

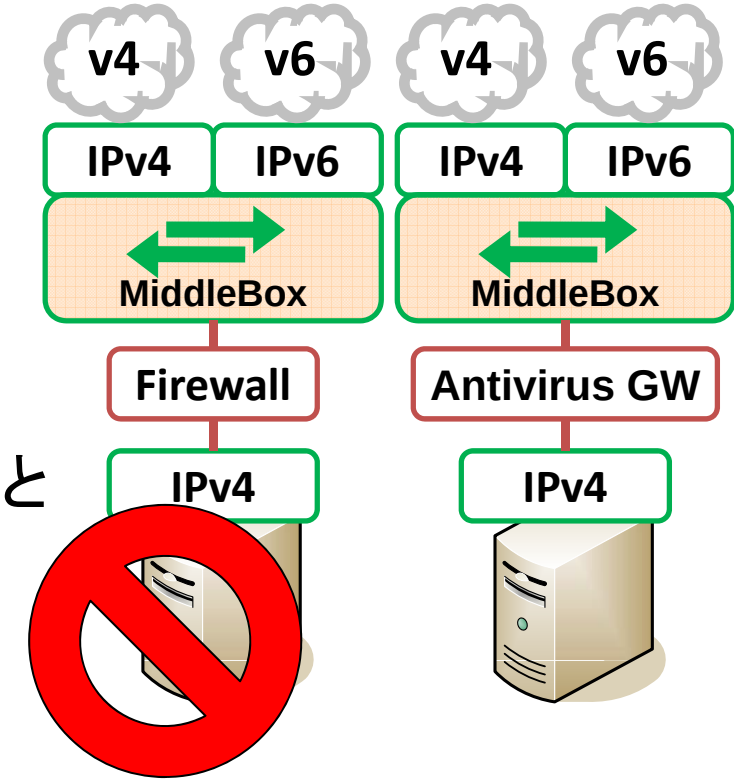
IPv4シングルスタック＋ミドルボックス



ミドルボックス構成上の課題

» ミドルボックス構成
  – サーバ自体はIPv4シングルスタック運用
  – ミドルボックスでIPv4/IPv6変換し、サービスはデュアルスタック

» 課題
  – Firewall, IDS/IPS, アンチウィルス ゲートウェイ等のセキュリティ機器の IPv6対応状況が課題
    • FirewallでIPv4/IPv6変換を行う方法も
  – IPv4のみに対応したセキュリティ機器と ミドルボックスを組み合わせる場合、 特に設置場所について配慮が必要



ミドルボックス運用時の課題

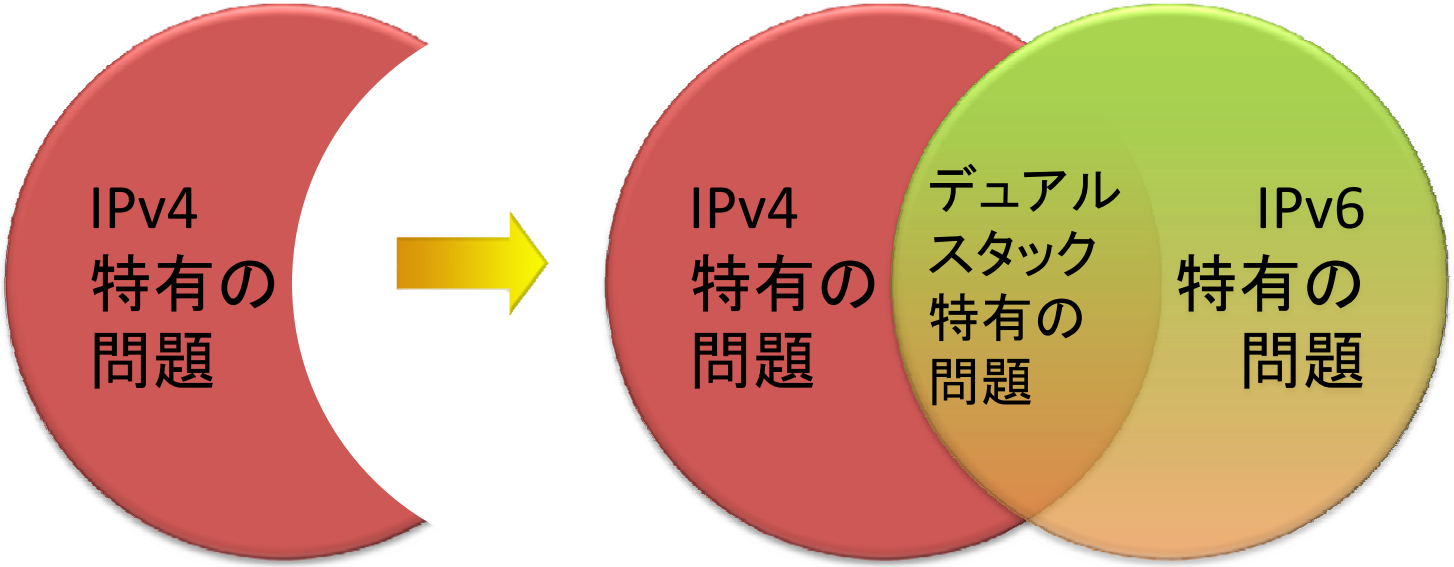
» サーバ
  – クライアントのIPアドレスに基づくアクセス制限が効かなくなる
  – IPv6からのアクセスは全てミドルボックスのアドレスに
    • サーバ側ではDoS攻撃などの対応能力が制限される

» ミドルボックス
  – アクセス制御
    • 必要なサーバ宛の通信のみを中継する
  – ログ取得
    • IPv4/IPv6変換前後のアドレスをつきあわせられる仕組みが必要

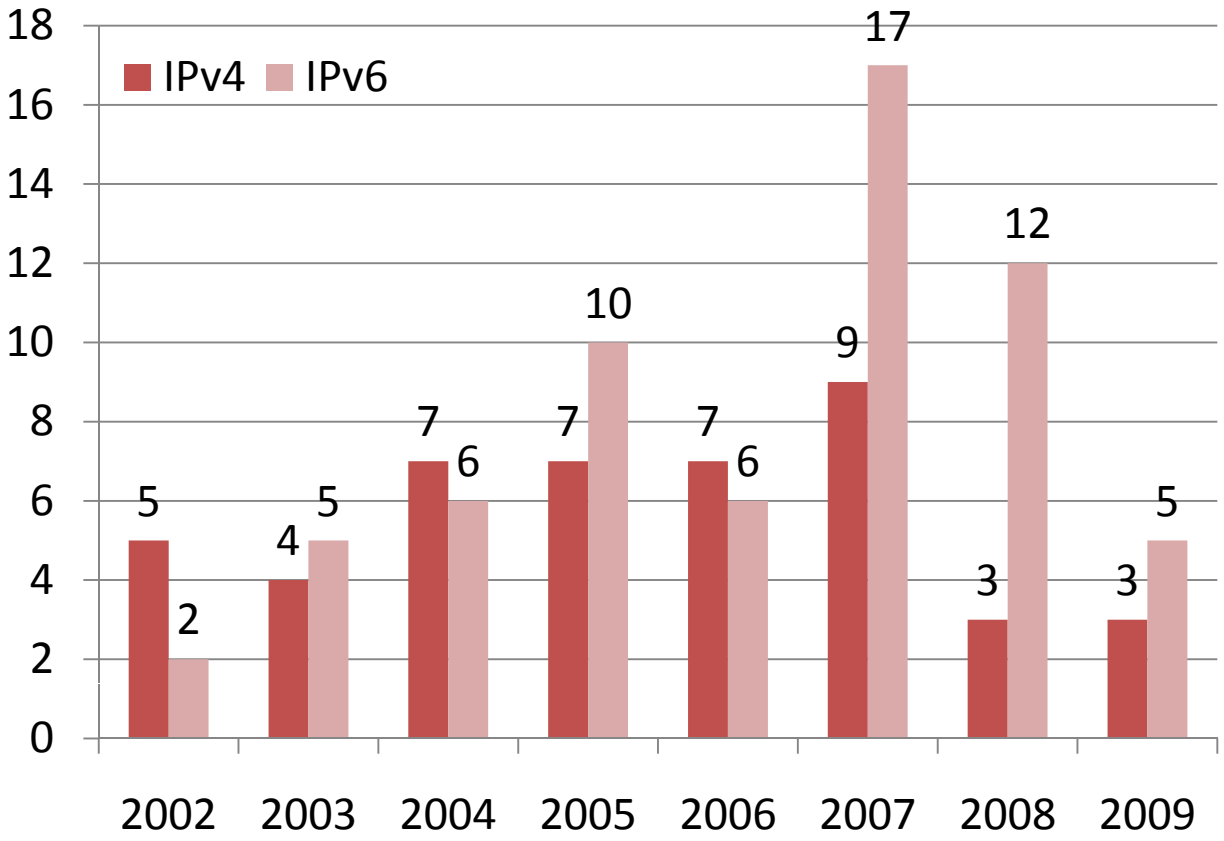
IPv4/IPv6プロトコルスタックの脆弱性の傾向

サーバのデュアルスタック対応

» IPv6を実装したソフトウェアは、IPv4に比べ歴史が浅いため何らかの欠陥が残っている可能性が高い



IPv4/IPv6 プロトコル特有の脆弱性の推移

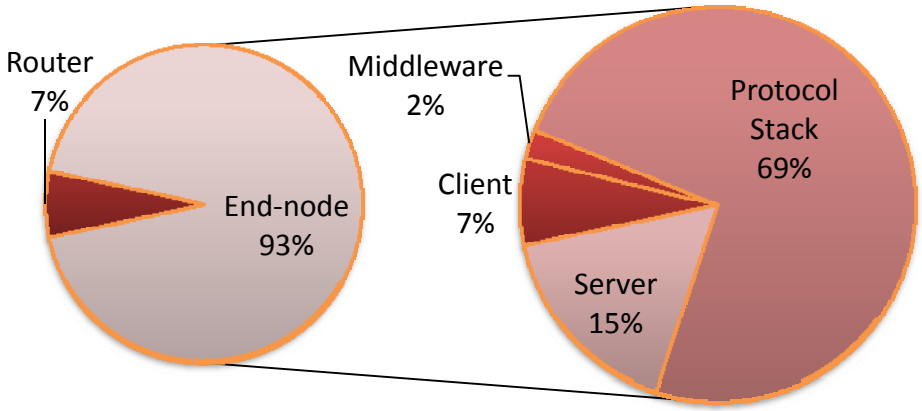


出典 : MITRE社の CVE Database より発表者が作成, 2009年5月現在

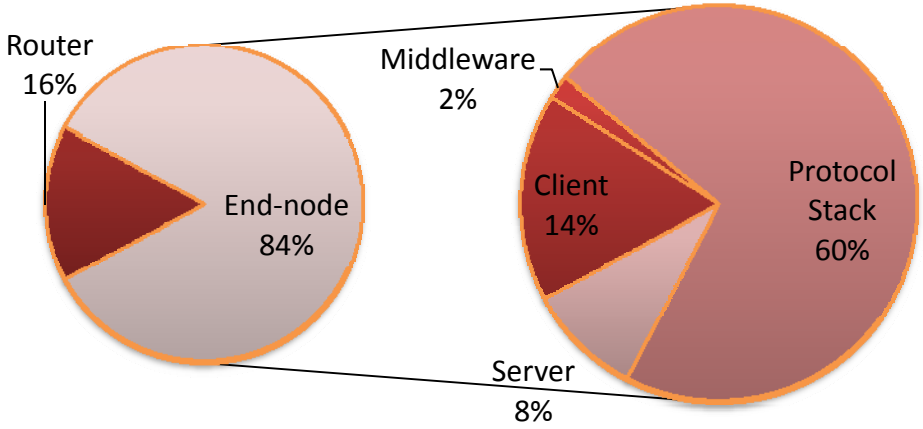
2007年以降に登録されたIPv6環境特有の脆弱性はIPv4環境特有の脆弱性の約2倍

IPv4/IPv6に関連した脆弱性の傾向

IPv4



IPv6



- プロトコルスタックの脆弱性が多い
- 個々のサーバ、クライアントアプリケーションも無視できない
- 脆弱性の例
  - [IPv4関連] 不正な形式のパケット処理に関する問題
  - [IPv6関連] IPv6アドレスの解釈時の問題

まとめ

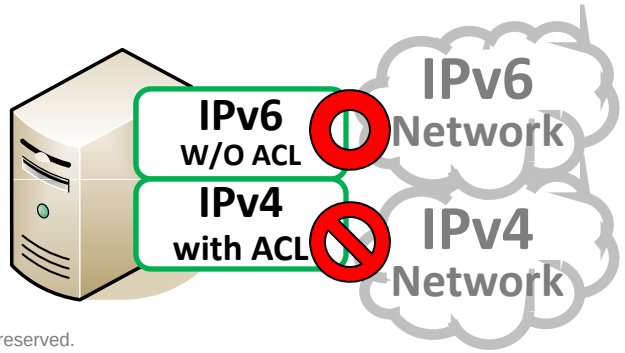
サーバのIPv6対応にあたって注意するべきポイント

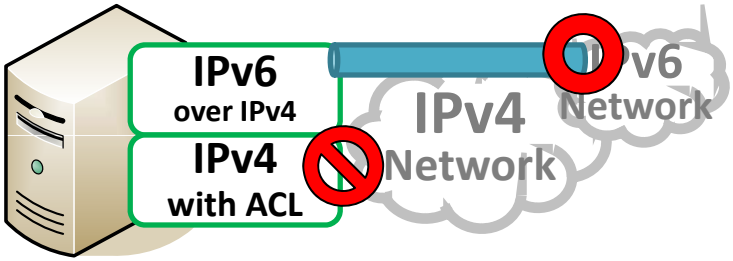
- IPアドレスの書式とログ取得
  - IPv4アドレス
  - IPv6アドレス
  - 特殊なIPv6アドレス
    - IPv4射影アドレスを用いる場合、IPv4アドレスの書式が「192.0.2.1」から「::ffff:192.0.2.1」となる
    - 例: あるPOP before SMTPサーバは、ログに記録されるIPv4アドレス形式が正規表現にマッチしないため、動作しなくなった
- アクセス制御
  - IPv4 と同じレベルのアクセス制御が IPv6 に対しても行われているか
  - 多くの実装では、IPv4アドレスの表記による設定でIPv4射影アドレスに対してアクセス制限が行われる
    - 一部の実装では、IPv4射影アドレスの表記による設定を行わないとアクセス制限が実施されない場合もある(古い実装に多い)

設定の対称性

» IPv4/IPv6いずれのプロトコルにおいても、同様のセキュリティレベルを確保することが望ましい
  – [例1] アンチウィルスゲートウェイを用いてIPv4のメールトラフィックにはウィルススキャンを実施しているが、IPv6に未対応のためスキャンされない
  – [例2] IPv4トラフィックにはパケットフィルタリングを実施しているが、IPv6トンネル内のIPv6パケットに対するフィルタリングが不十分

» セキュリティ機器のIPv6対応状況も要確認
  – IPv4/IPv6変換用のミドルボックスとIPv4のみに対応したセキュリティ機器を併用する場合には、トポロジを工夫
  – IPv6とIPv4で実装されている機能に差がある場合が多い





課題のまとめ

- デフォルト設定、自動設定に注意が必要
  - 必要なプロトコルだけを有効にする
    - IPv4だけを利用しているつもりでもIPv6が有効になる可能性がある
- IPv4/IPv6デュアルスタック
  - OSやアプリケーションの種類、設定により、ソケットの実装やIPv4射影アドレスの動作が異なるため、確認が重要
  - IPv4シングルスタック運用からIPv4/IPv6デュアルスタック運用に変更した場合に、潜在的な脆弱性が増加する可能性がある
- IPv4シングルスタック+ミドルボックス
  - IPアドレスに基づくアクセス制御が難しくなる
  - FirewallやIPSなど、セキュリティ装置の設置場所について配慮が必要
- セキュリティリスクや短期的な改修コストと将来性、運用コストなどの総合的な考慮が必要