Internet Week 2011

2011年12月1日

T-4 : 13:00 – 15:30

IPv6セキュリティの勘どころ
企業ネットワークでのIPv6セキュリティ

2011年12月1日

ネットワンシステムズ株式会社

ビジネス推進G　マーケティング本部

ソリューション・マーケティング部　第2チーム

花山　寛

hanayama at netone.co.jp

Net One Systems　Net One Partners　Business Assurance Co.,Ltd.

すべてのステークホルダーから信頼され支持される企業へ
ADMIRED COMPANY

プロフィール

- 1996年　ネットワンシステムズ株式会社　入社
- 1997年　マーケティング本部 プロダクトマーケティング部にてATM/FR交換機、MPLS製品ならびにVoIP製品に関わるプロダクトマーケティングに携わる
- 2001年　応用技術部にてソフトウエア/製品/サービス/ソリューション開発にて、新技術をベースとしたソフトウエア/製品/サービス開発、セキュリティ調査などに携わる
- 2009年　NWテクノロジー本部　研究開発部　リサーチチームにて、新技術に関する調査研究ならびにテクニカルマーケティングに携わる
- 2011年　マーケティング本部　ソリューションマーケティング部　所属
  新世代、データセンター、クラウド、仮想化に関連する最新技術などのテクニカルマーケティングと共に、主にIPv6に関連する各種社外団体の活動に参加
- 社外活動など
  - インターネット協会　IPv6ディプロイメント委員会
  - IPv6普及･高度化推進協議会
  - IPv4アドレス枯渇対応タスクフォース
  - 日本ネットワークセキュリティ協会
  - 日本データセンター協会
  - など

Agenda

- IPv6市場動向
- IPv6ネットワークとセキュリティ
- 課題の解説と脅威の対策
- IPv6導入事例紹介
- 仮想化時代のIPv6セキュリティ
- まとめ

会場の皆様への質問

はじめる前に - 1

現在のステータス

1：IPv6ネットワークの導入を検討中
2：IPv6ネットワークの導入を計画中
3：IPv6ネットワークの導入を準備中(構築の)
4：IPv6ネットワークの構築中
5：IPv6ネットワークの運用中

はじめる前に - 2

導入時期(予定を含む)

1：2010年

2：2011年

3：2012年

4：2013年

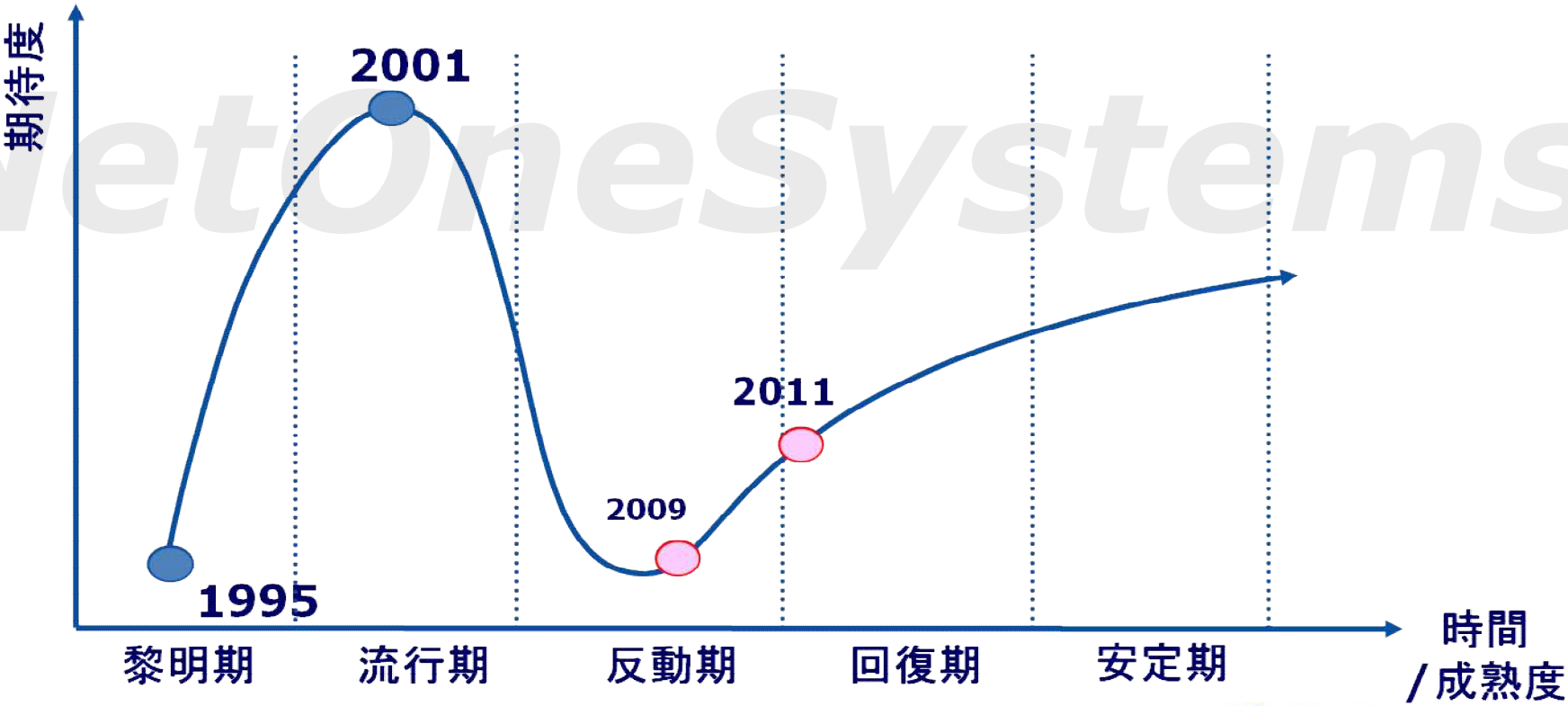
5：2014年

IPv6市場動向

ハイプサイクル

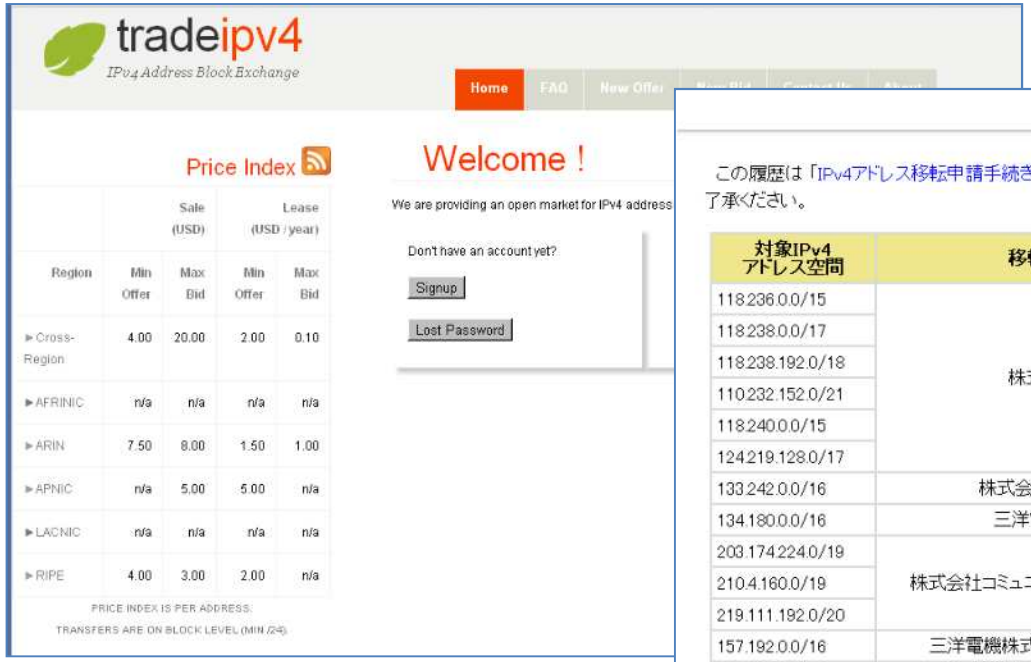
IPv6に特化したハイプ・サイクル　※私見

- ガートナー社がテクノロジーなどの期待度・成熟度を示す場合に用いる
- 縦軸にユーザーやメディアの期待度・認知度,横軸に時間・成熟度を設定した座標に曲線の形で表現され、この上に当該技術がどのフェイズにあるかをマッピング



IPv4アドレス移転

既に始まっている



IPv4アドレス移転履歴(2011年11月21日現在)

この履歴は「IPv4アドレス移転申請手続き」に基づき公開するものです。JPNICでは下記の移転履歴に関するお問い合わせには応じられませんので、あらかじめご了承ください。

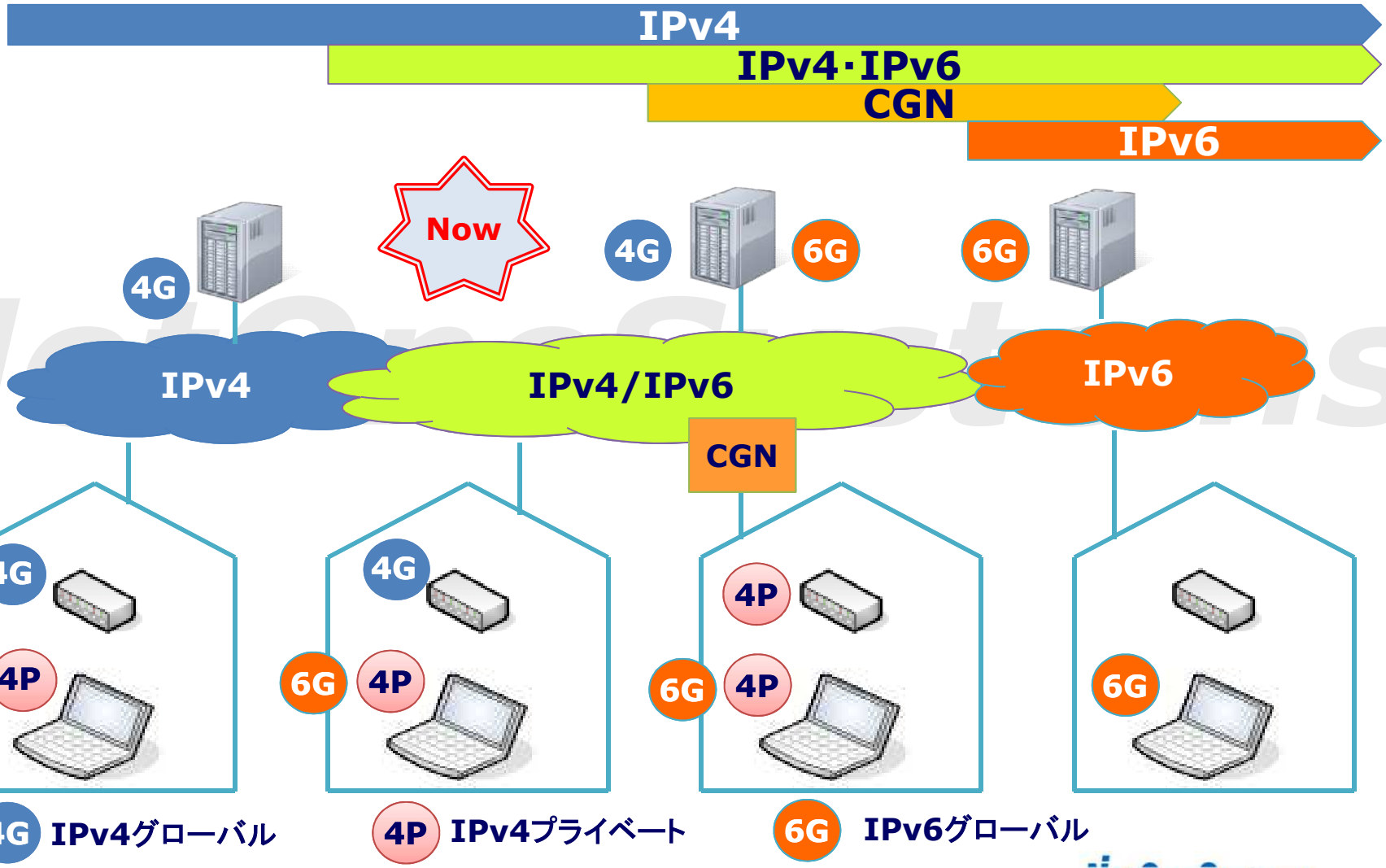
対象IPv4アドレス空間	移転元組織名	移転元組織への割り振りまたは割り当て日	移転先組織名	移転日
118.236.0.0/15	株式会社USEN	2007-11-05	ソネットエンタテインメント株式会社	2011-08-22
118.238.0.0/17		2007-11-05		
118.238.192.0/18		2007-11-05		
110.232.152.0/21		2009-05-26		
118.240.0.0/15		2007-11-06		
124.219.128.0/17		2007-11-06		
133.242.0.0/16	株式会社建築システム	1990-09-03	さくらインターネット株式会社	2011-08-29
134.180.0.0/16	三洋電機株式会社	1994-02-28	三洋ITソリューションズ株式会社	2011-09-20
203.174.224.0/19	株式会社コミュニティネットワークセンター	2004-06-03	KMN株式会社	2011-10-11
210.4.160.0/19		2006-05-08		
219.111.192.0/20		2002-07-30		
157.192.0.0/16	三洋電機株式会社 ITシステム本部	2010-03-30	三洋ITソリューションズ株式会社	2011-10-31
202.241.128.0/22	株式会社TCP	1995-03-23	株式会社インターリンク	2011-11-01
202.241.136.0/22				
202.241.144.0/21				
202.241.152.0/22				
202.241.180.0/22		1996-08-14		
157.14.96.0/19		1991-12-10		
157.14.136.0/21				
157.14.144.0/20				
157.14.208.0/22				
157.14.252.0/22				
202.255.16.0/21	徳島県立二十一世紀館	1994-08-09	株式会社STNet	2011-11-21

出典 http://tradeipv4.com/

出典 http://www.nic.ad.jp/ja/ip/ipv4transfer-log.html

今後のインターネット

IPv4/IPv6ネットワーク･CGNの混在ネットワーク

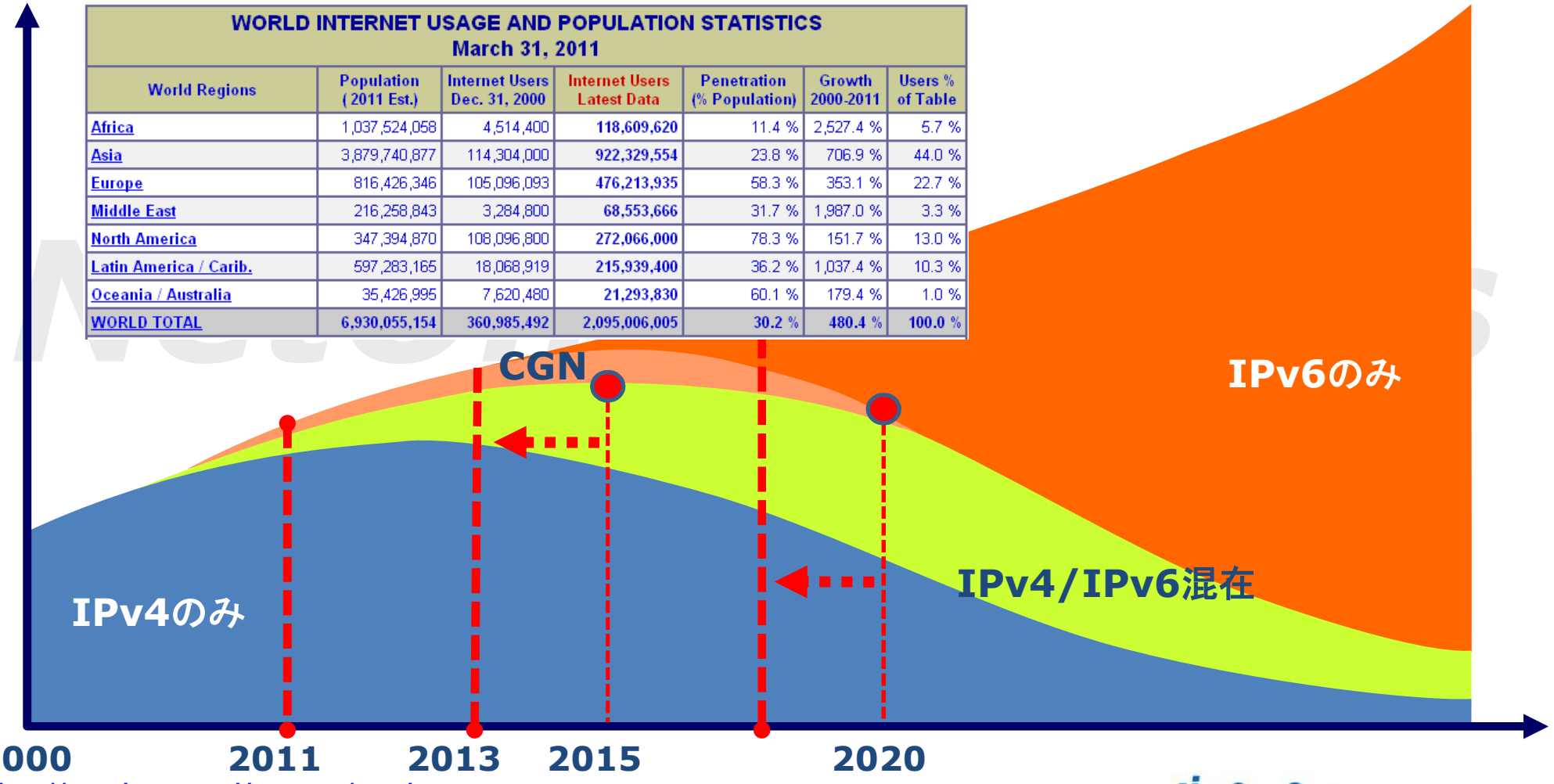


IPv6導入、移行の予測　※私見

- 世界のインターネット人口：約21億人　*: 2011年3月31日
- 世界人口　70億人突破　*:2011年10月31日

WORLD INTERNET USAGE AND POPULATION STATISTICS
March 31, 2011

World Regions	Population (2011 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2011	Users % of Table
Africa	1,037,524,058	4,514,400	118,609,620	11.4 %	2,527.4 %	5.7 %
Asia	3,879,740,877	114,304,000	922,329,554	23.8 %	706.9 %	44.0 %
Europe	816,426,346	105,096,093	476,213,935	58.3 %	353.1 %	22.7 %
Middle East	216,258,843	3,284,800	68,553,666	31.7 %	1,987.0 %	3.3 %
North America	347,394,870	108,096,800	272,066,000	78.3 %	151.7 %	13.0 %
Latin America / Carib.	597,283,165	18,068,919	215,939,400	36.2 %	1,037.4 %	10.3 %
Oceania / Australia	35,426,995	7,620,480	21,293,830	60.1 %	179.4 %	1.0 %
WORLD TOTAL	6,930,055,154	360,985,492	2,095,006,005	30.2 %	480.4 %	100.0 %



出典 http://www.internetworldstats.com/stats.htm

IPv6導入・検討　意識調査など

Cisco：米国内のIT企業101社に対する調査

- 78%の組織が、IPv6への移行を行ったか、現在計画中であると回答
- IPv6移行作業の94%が、過去2年以内に開始
- 開始していない人は、作業開始前に最低9ヶ月間の調査

出典 http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=296429
出典 http://www.soumu.go.jp/main_content/000124348.pdf

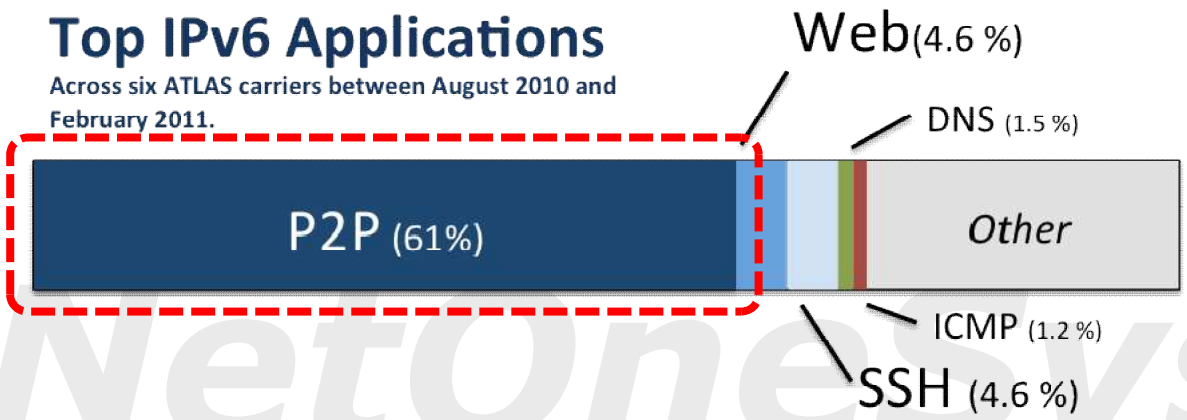
Network World：200以上の米企業のIT専門家に対する最新の調査結果

- 企業の7割以上は2013年までにIPv6に対応させると回答

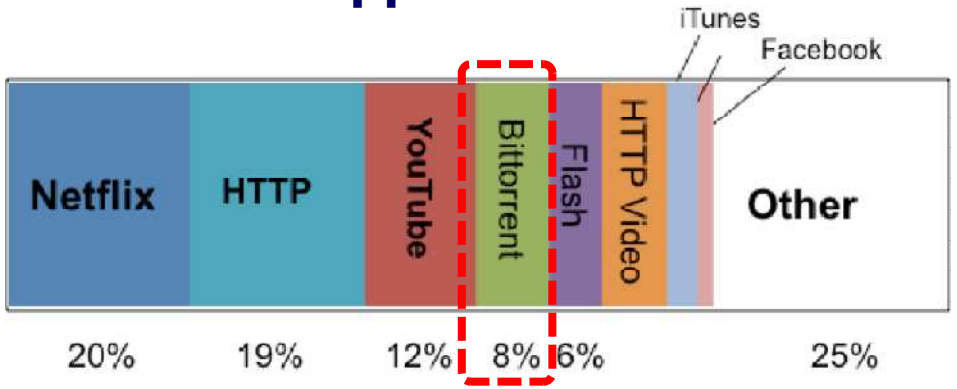
出典 http://www.networkworld.com/news/2011/072611-ipv6-survey.html
出典 http://www.networkworld.com/slideshows/2011/nww-ipv6-survey-ciscosubnet.html

IPv6トラフィックの傾向から考える対応と措置

2010年8月 – 2011年2月の測定結果



IPv4 Application Traffic

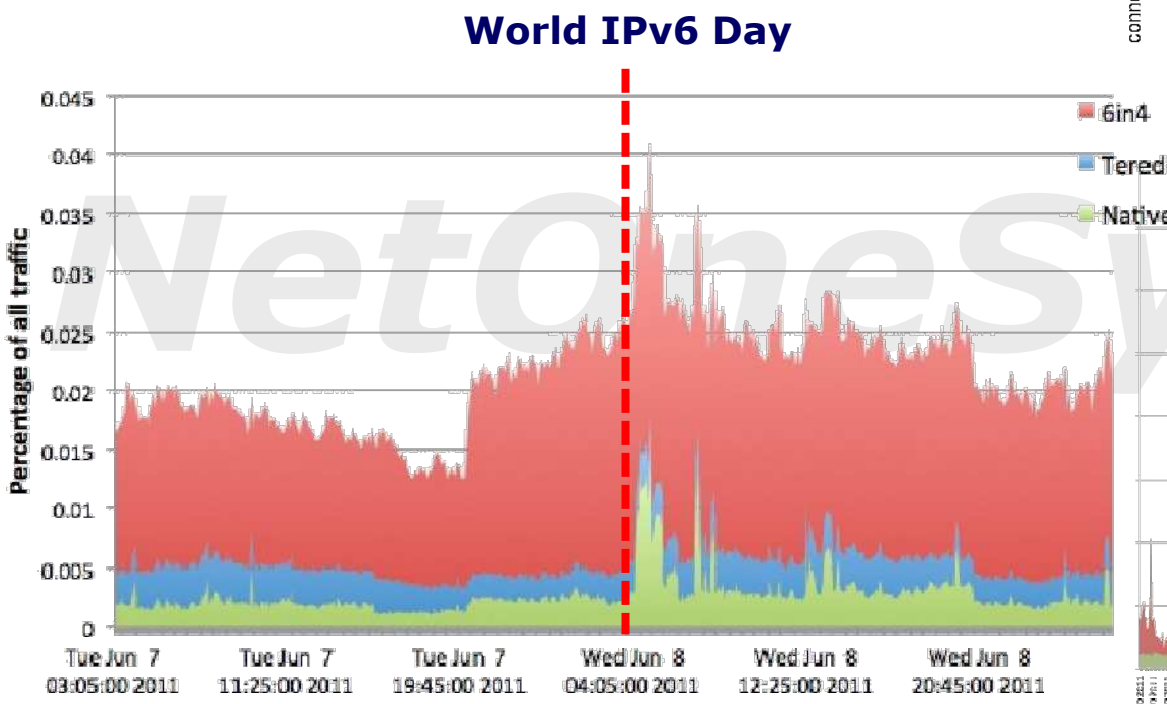


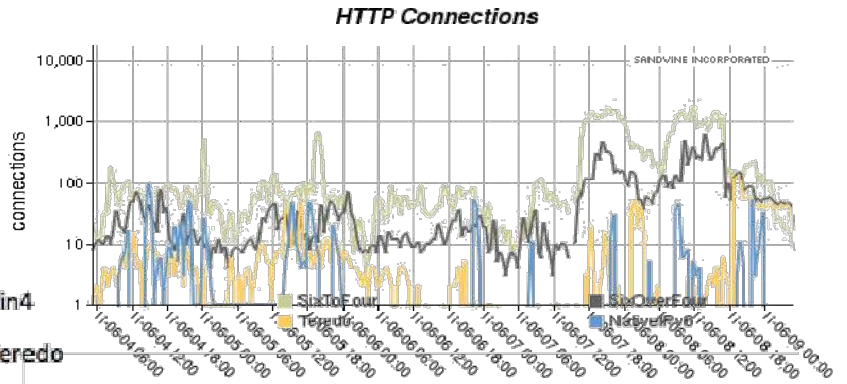
出典 http://asert.arbornetworks.com/2011/04/six-months-six-providers-and-ipv6/

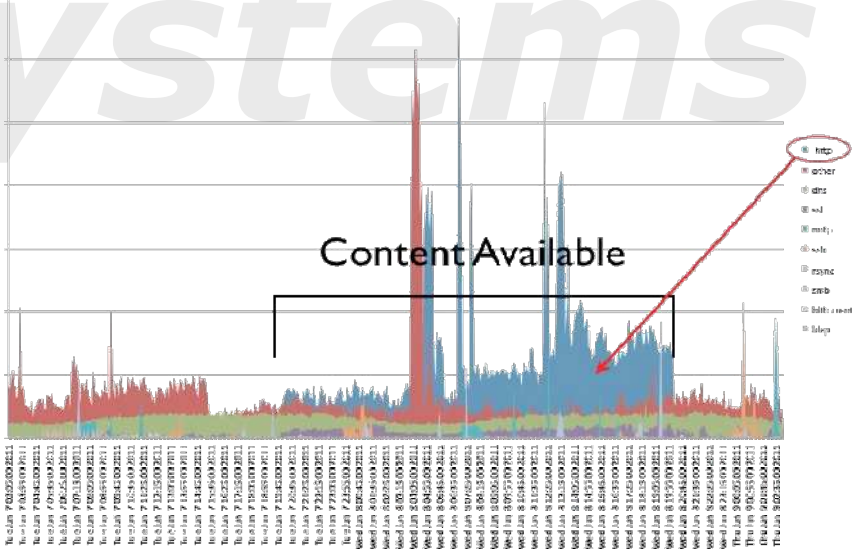
IPv6トラフィックの変化

2011年6月8日

World IPv6 Day





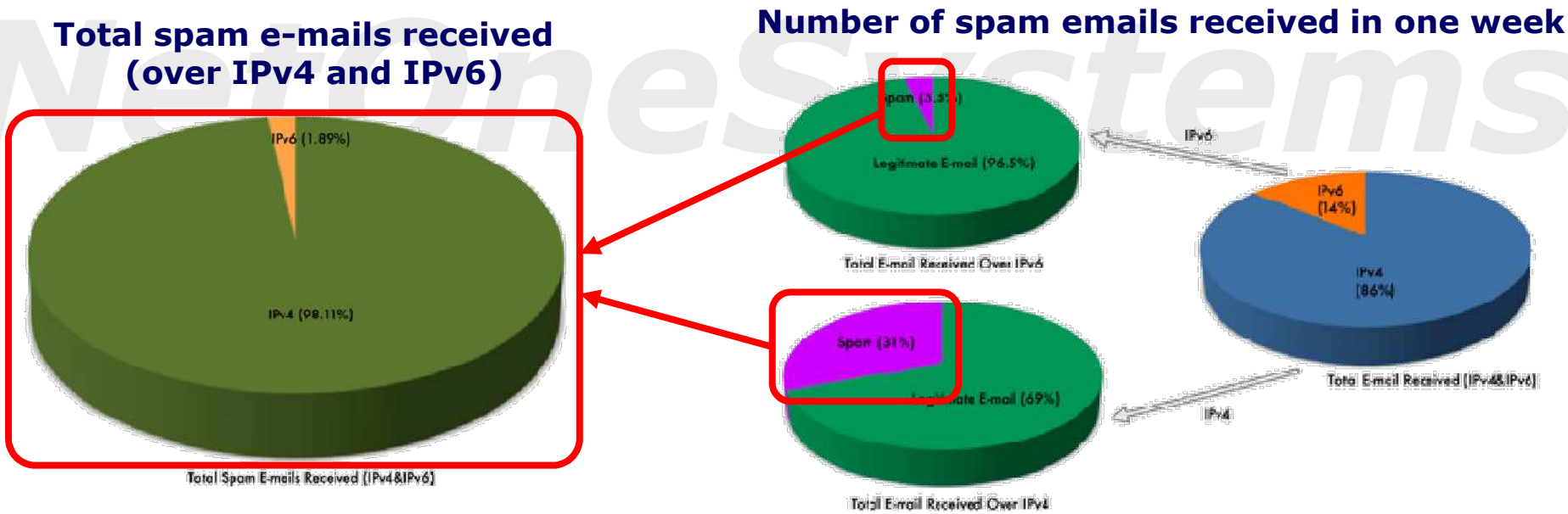


出典 http://www.betterbroadbandblog.com/2011/06/world-ipv6-day-%E2%80%93-sandvine-policy-traffic-switch-records-a-smooth-test-flight/

出典 http://asert.arbornetworks.com/2011/06/world-ipv6-day-final-look-and-wagons-ho/

IPv6 Spam (bot)

- 意図的にIPv6を利用しているというわけではなく、知らぬ間に･･･?
- 受信側のメールサーバのアドレスのAAAAの応答があればIPv4経由だったスパムがIPv6経由で･･･?
- 利用しているホスティングサービス等がIPv6に対応している場合、受信側のメールサーバがIPv6対応とAAAAレコードの応答があれば･･･?



出典 https://labs.ripe.net/Members/blazquez/content-spam-over-ipv6

Gartnerの予測

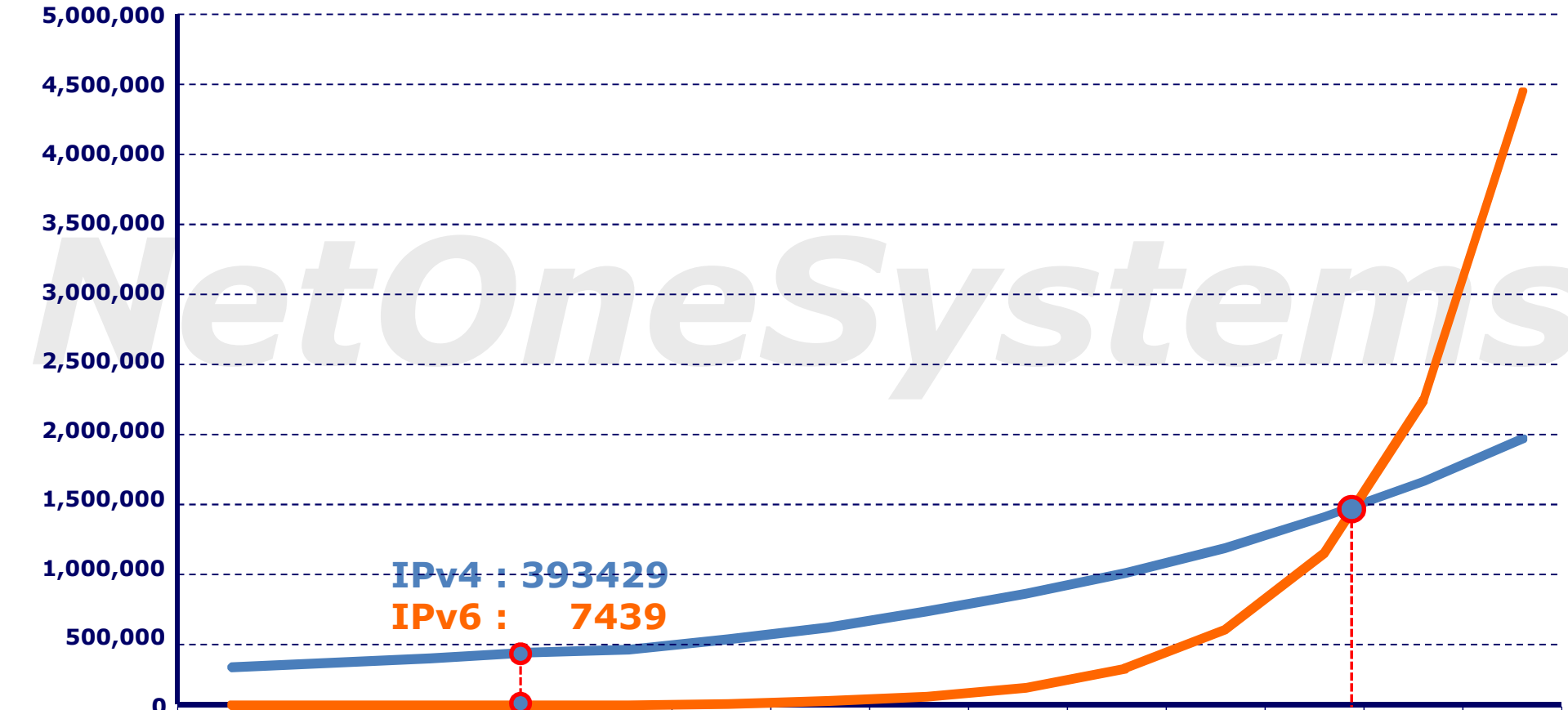
- 2011年末には、世界で利用されるPCの42%が「Windows 7」搭載機になる
- 2011年に出荷される新規PCのうち94%がWindows 7を搭載するとも予想
- 2011年末までには、世界の約6億3500万台の新規PCがWindows 7を搭載して出荷されると予想
- 2011年末には、Mac OSは世界のPCの中で4.5%のシェアを占める
- Googleの「Chrome OS」と「Android」、（Hewlett-Packardの）「webOS」は今後5年間、PC市場において大きなシェアを獲得しないだろう

出典 http://japan.cnet.com/sp/allaboutms/35006101/

IPv4/IPv6 フルルートの変化と予測

増加率：IPv4 18.9%,IPv6 101.1%

*:Geoff Hustonのデータから増加率,手法はcidrv6を適用

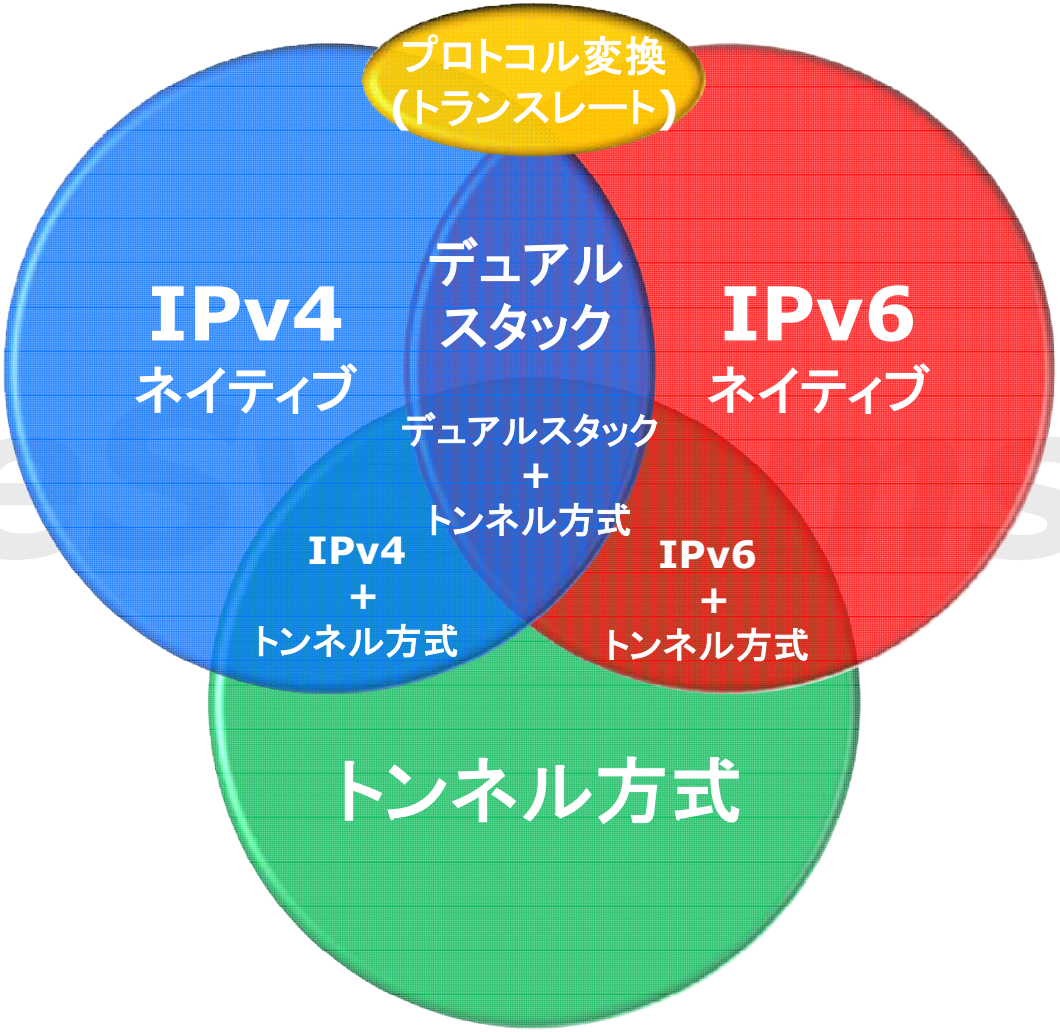


	2009年1月	2010年1月	2011年1月	Today	2012年1月	2013年1月	2014年1月	2015年1月	2016年1月	2017年1月	2018年1月	2019年1月	2020年1月	2021年1月
IPv4フルルート	284,194	312,989	341,483	393,429	405,974	482,644	573,794	682,158	810,986	964,145	1,146,229	1,362,700	1,620,053	1,926,008
IPv6フルルート	1,596	2,458	4,100	7,439	8,245	16,582	33,347	67,064	134,869	271,230	545,460	1,096,955	2,206,045	4,436,495

IPv6ネットワークとセキュリティ

IPv6導入モデルの整理

- パラレル･スタック
- デュアル･スタック
- トンネル
- トランスレート



内閣官房情報セキュリティセンター

政府機関の情報セキュリティ対策のための統一技術基準

2.4.1.1 情報システムへのIPv6 技術の導入における対策

遵守事項

(1) IPv6移行機構がもたらす脆弱性対策

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、情報システムにIPv6技術を利用する通信（以下「IPv6通信」という。）の機能を導入する場合には、IPv6移行機構が他の情報システムに情報セキュリティ上の脅威を及ぼすことを防止するため、必要な措置を講ずること。

(2) 意図しないIPv6 通信の抑止と監視

【基本遵守事項】

(a) 情報システムセキュリティ責任者は、IPv6通信を想定していない通信回線に接続されるすべての電子計算機及び通信回線装置に対して、IPv6通信を抑止するための措置を講ずること。

【強化遵守事項】

(b) 情報システムセキュリティ責任者は、IPv6 通信を想定していない通信回線を監視し、IPv6通信が検知された場合には通信している装置を特定し、IPv6通信を遮断するための措置を講ずること。

出典：内閣官房情報セキュリティセンター 政府機関の情報セキュリティ対策のための統一技術基準
http://www.nisc.go.jp/active/general/pdf/K305-101.pdf

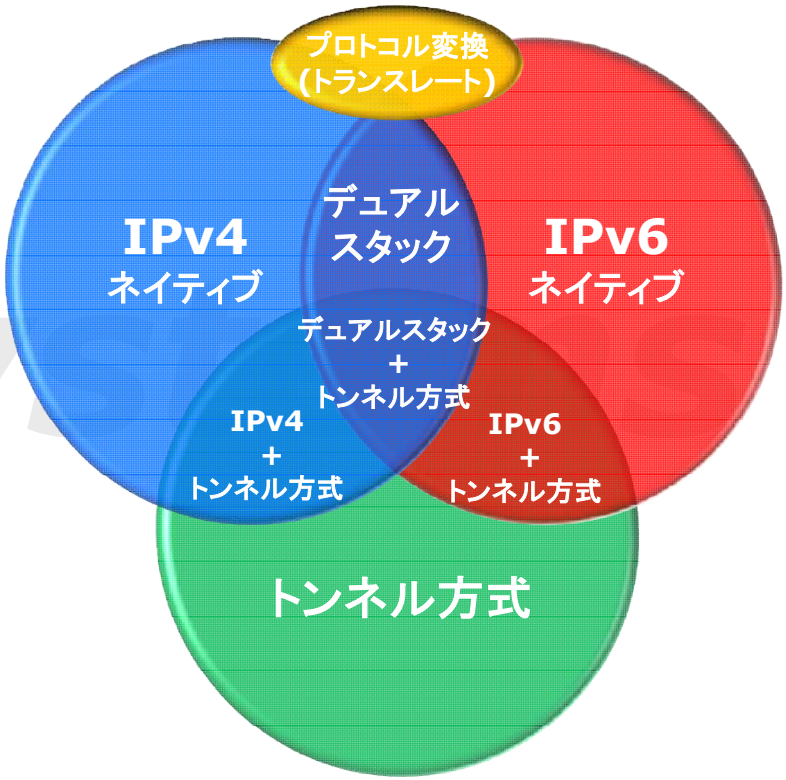
IPv6導入とセキュリティ

IPv6移行機構がもたらす脆弱性対策

- 不正なルータ広告による通信不全
- ステートレス自動設定(SLAAC)に関する問題
- マルチキャストに関する問題
  - 組織スコープのマルチキャストの悪用
  - ICMPv6 のエラー返答の悪用
- 経路制御ヘッダ利用によるアクセス・フィルタの回避
- 中継点オプション・ヘッダの悪用
- 他の問題
  - プライバシーアドレス

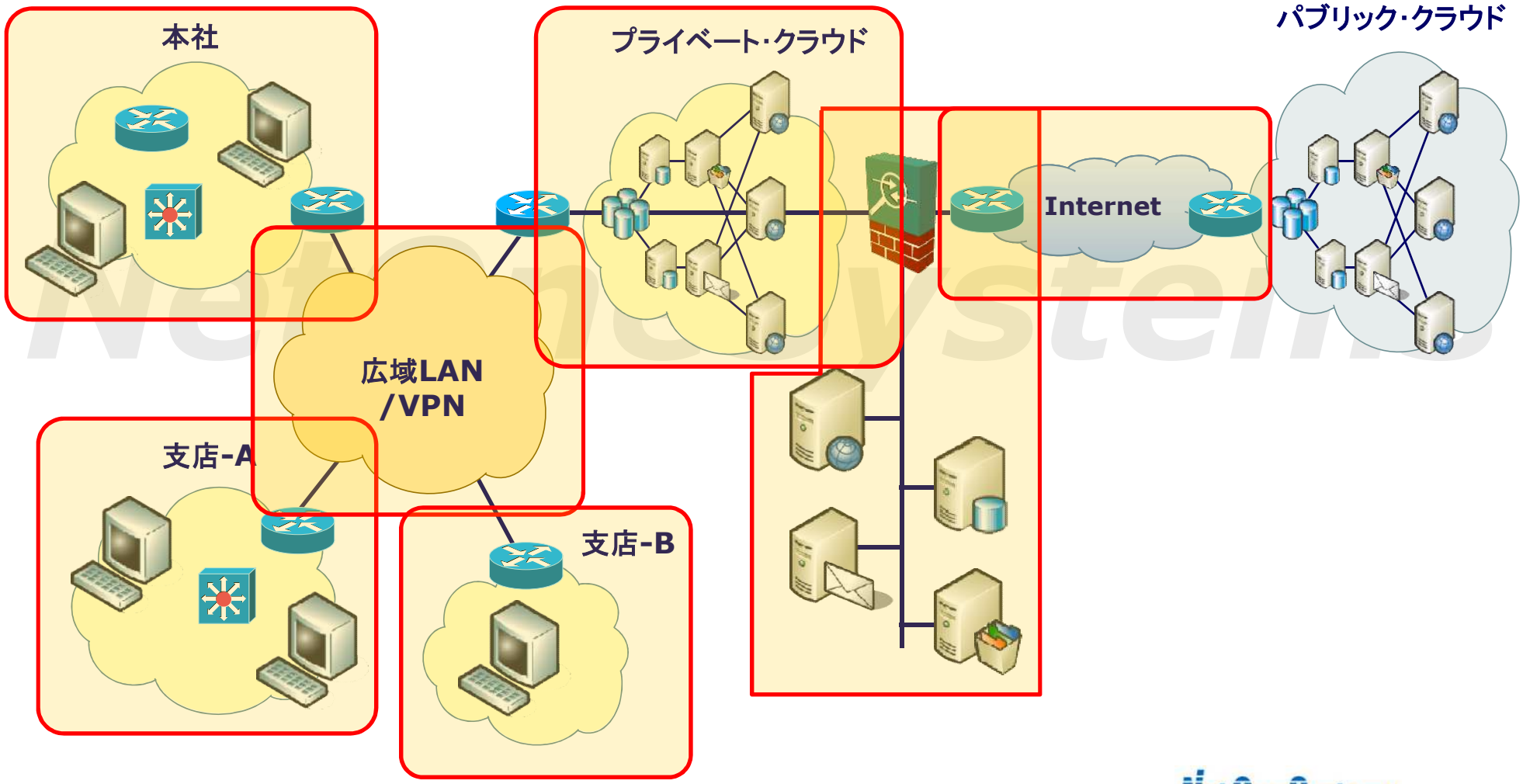
意図しないIPv6通信の抑止と監視

- 不正なルータ広告による通信不全
- 自動トンネル機能
  - 6to4,TeredoなどのIPv6トンネル接続
  - アプリケーションによってはP2P接続に利用
- FirewallのIPv6トンネル接続ルールの追加
- モニタリングによる対策
  - セグメント内のNDPパケットの異常を検知



ネットワーク･モデルと留意箇所

企業システム例と構成要素



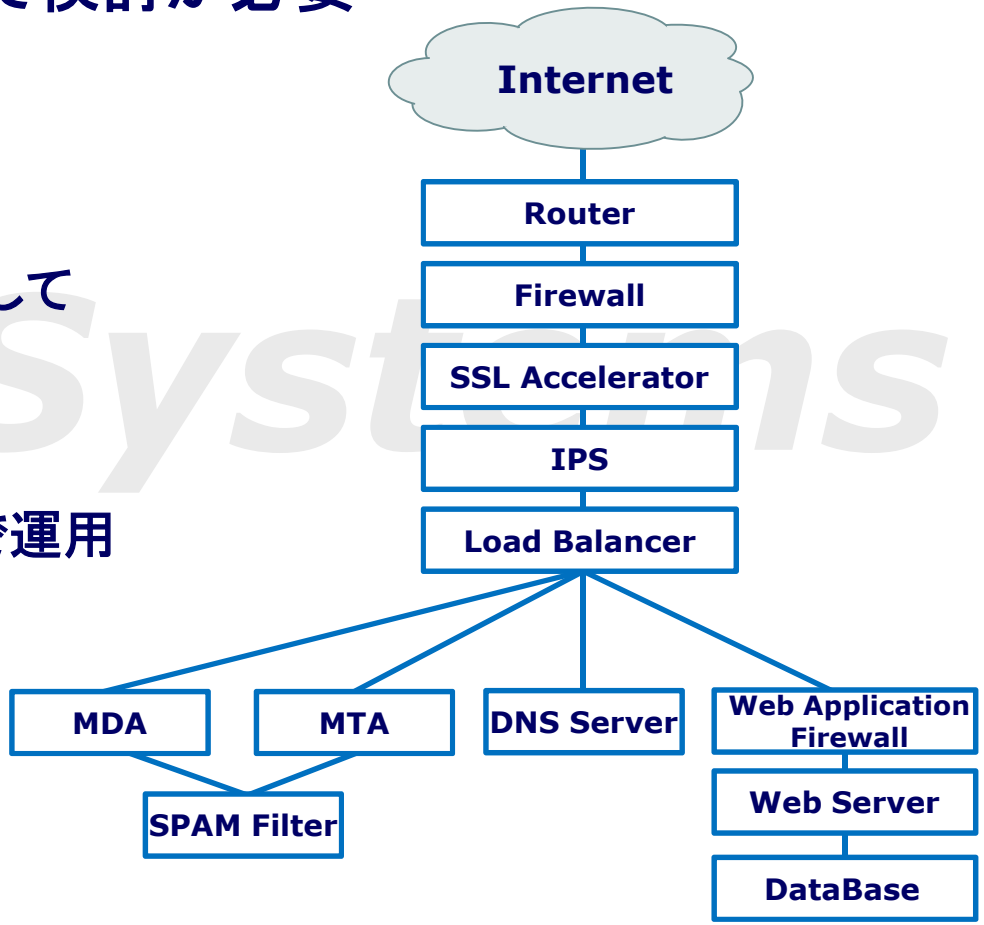
企業のIPv6セキュリティの分類と留意点

- インターネット･アクセス
  - 通信事業者の対応、ISPのサービス品目、回線、
  - デュアルスタック、トンネル、DNS、アドレス、
- DMZ
  - 機器対応/実装/組み合わせ、
  - 接続構成、アドレッシング、フィルタリング、ログ、マネージメント、
  - Webアプリ、ネットワークアプリケーション、アプリケーション開発言語、
- 本社、支店
  - クライアントOS、アプリケーション、
  - ルーティング、アドレッシング、セグメンテーション、
- プライベートクラウド(計算機センター)：サーバファーム
  - サーバOS、アドレッシング、仮想化、
  - バックアップ、ログ、マネージメント、
  - Webアプリ、社内専用/市販アプリケーション、
- 広域LAN/VPN
  - サービス内容、L2アクセス、VPNアクセス、

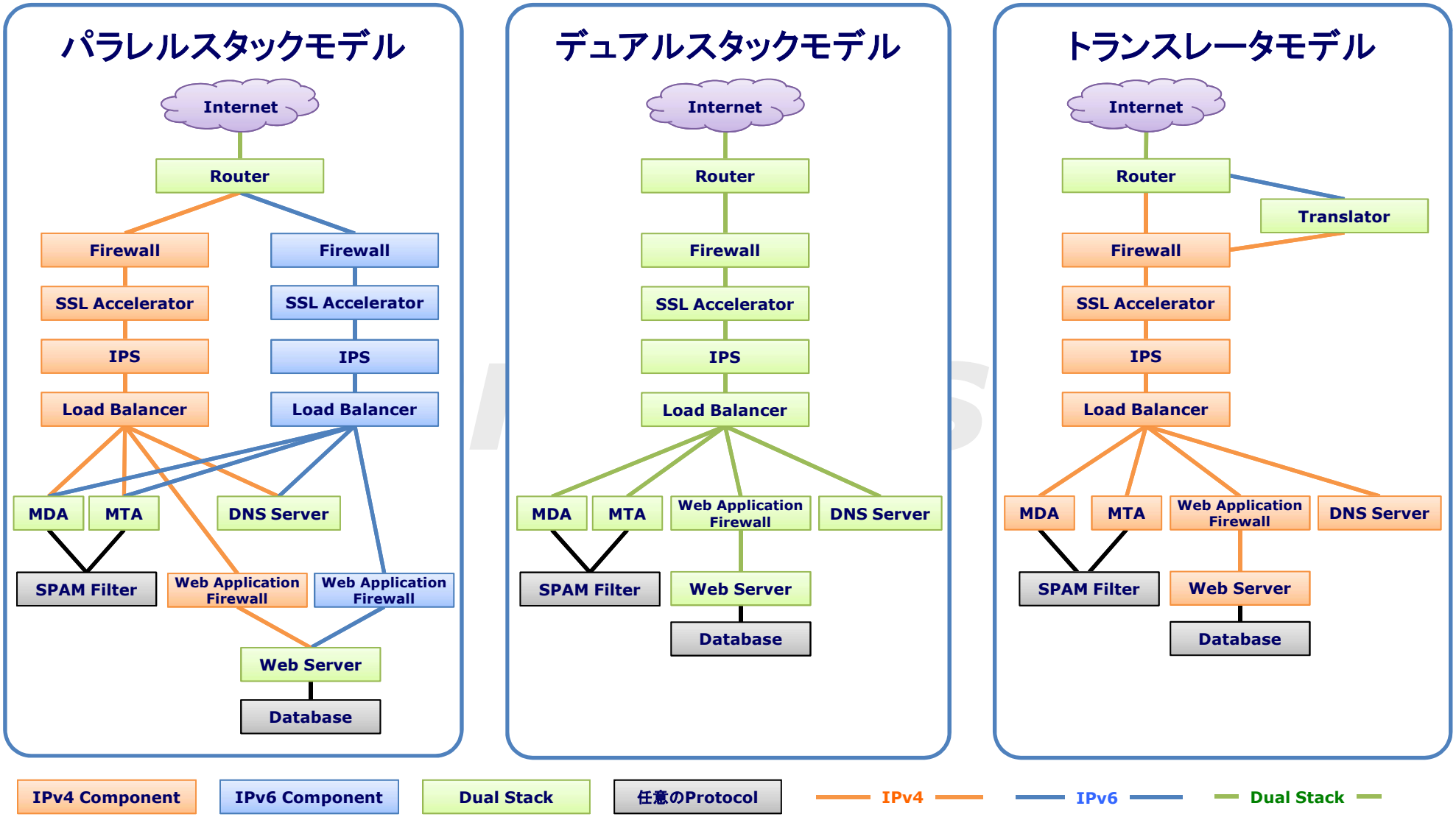
一般企業の概念的なDMZの構造と導入モデル

- IPv6対応はデュアルスタックだけではない
- 導入セグメントの性質に注意して検討が必要

- 3つの導入モデル
- パラレルスタックモデル
  - IPv6ネットワークをIPv4と独立して導入するモデル
- デュアルスタックモデル
  - 機器をIPv6対応し両プロトコルで運用するモデル
- トランスレータ
  - IPv4ネットワークを変更せずトランスレータによりIPv6対応をするモデル



3つの導入モデルの比較（DMZの）



導入モデルにおける注意事項

各モデル毎のメリット/デメリット

	パラレル	デュアルスタック	トランスレータ
メリット	• 分岐点が明確 • 概念が単純 • 実績の少ないネットワークの分離が可能 • 導入・移行が容易	・新規投資が少ない	・新規投資が少ない ・ネットワーク構造の変化が少ない
デメリット	• 初期投資が多い • 管理対象が増す	• セキュリティ機器の実績が乏しい • ネットワーク構造を変更する必要がある • 分析・管理工数が増加 • 障害時の影響範囲が広い	• 実績が非常に少ない • 障害発生時の対応が比較的難しい • セキュリティ機器の通信制御が難しい

IPv6 Security Products List/Tests

- ICSA Lab October 6, 2010
  - 製品のIPv6実装状況
  - https://www.icsalabs.com/technology-program/ipv6/ipv6-capable-security-products
- IPv6 to Standard
  - 各製品のRFC対応状況
  - http://www.ipv6-to-standard.org/

- 日本セキュリティオペレーション事業者協議会(ISOG-J)
  - Firewall,IPSなどの検証報告書
  - IPv6検証報告書
    http://www.jnsa.org/isog-j/output/2011/ISOG-J_IPv6_Verification_Report.pdf

機器選択時のポイント -1

- 「IPv6対応」と明記されていても実装内容が個々に異なる
- IPv6対応
  - ソフトウエア、ハードウエア(ASIC)の2種類
  - 当初はソフトウエア対応でも、ファームVerUpなどでH/W対応になるものもある
- 処理性能
  - IPv4と同等の処理性能を持たないのものある
  - ソフトウエア対応(処理)の場合、処理性能が低いこともある
  - 機能の組合せにより処理性能が異なることもある
  - デュアルスタックで動作させると期待通りの処理性能が出ないこともある
- 冗長性
  - 対応していないもがある *:VRRP Ver3.0でIPv6対応
  - 切り替え時にセッションを維持できないこともある *:テーブルの保持が出来ない
  - デュアルスタックはシングルスタックに比べ切替が遅れることがある
  - アクティブ-アクティブなどの構成が不可能なものもある

機器選択時のポイント-2

運用管理

- 管理ポートにIPv6アドレス設定が出来ない
- IPv6ログの出力が出来ない
- IPv6ログの表示形式が機器、Ver毎に異なることもある
- IPv6 MIBに対応していないものもある
- IPv6 MIBの取得をIPv4で行うこともある
- IPv6コマンド(ping,telnet,ssh,ftp,ntp,etc)に対応していないこともある

その他

- IPv6でVerUp,シグネチャなどの各種アップデートが出来ない
  - IPv6での通信は可能だが、サーバ(サービス)が未対応の場合もある
- グローバルIPv4アドレスベースで取得(設定)したサーバ証明書は注意

IPv6アドレス管理、表現、など

- アドレス、システム管理、複数のログをクロス分析する場合や、ログを照合するような場合、モジュールや機能間の差分を吸収するために正規化処理が必要
- RFC4291は表記の柔軟性が高いため、同じアドレスでも異なる表記になり、誤解を招くことが多いと考えられることから注意が必要
- お勧め
  - 正規表現　*:一切省略しない
    - 2001:0db8:0000:0000:0001:0000:0000:0001

  or

  - RFC5952
    - 先行する “0” は必ず省略する　*:2001:0db8::0001の場合、2001:db8::1
    - “::” で省略する場合はできるだけ省略する　*:2001:db8:0:0:0:0:2:1の場合、2001:db8::2:1
    - 16ビットの0フィールドが1つの場合は省略しない　*:2001:db8:0:1:1:1:1:1は○、2001:db8::1:1:1:1:1は×
    - 16ビットの0が多いフィールドを省略する、同じ場合は前方を省略する　*:2001:0:0:1:0:0:0:1の場合、2001:0:0:1::1は○、2001::1:0:0:0:1は×
    - 英小文字("a", "b", "c", "d", "e", "f") を使う　*:大文字のDは0に、Bは8と間違え易い

課題の解説と脅威の対策

課題と脅威の整理

- 分類
  - 利用者 (中間者)
  - 管理者
- 状態
  - 気がつかない間に
  - 設定不足、誤操作など
- 事例
  - 事例-1 ： クライアント、サーバOSのIPv6設定が有効になっている
  - 事例-2 ： トンネル接続に気がつかない
  - 事例-3 ： 2つのネットワークI/Fが有効になっているPC、ICS (Internet Connection Sharing)が有効
  - 事例-4 ： ネットワーク機器へのフィルタなどの設定不足
  - 事例-5 ： オペレーションミス
  - 事例-6 ： 脅威/攻撃のターゲット、機器のセキュリティFixの未対応

新たな脅威とその整理

- IPv6ネットワークが増加するに従い、新たな脅威の発生が想定
- 特に、新たなアプリケーション/サービス利用時に発生
  - プロトコル、サービスそのもの脆弱性
  - セキュリティ対策の準備遅れ
  - 想定外の通信や利用方法
  - 利用者の盲点
  - さまざまな問題
- IPv6 について現段階で想定される攻撃利用対象
  - プロトコル実装における脆弱性
  - アプリケーション・脆弱性
  - マルウェアダウンロード,リダイレクト経路、情報流出経路としてIPv6の利用
- IPv6プロトコルに対する攻撃 *:IPv4のARP,DHCP,IGMP,ICMP Redirectに相当
  - DoS : NS/NA,RS/RA,DHCPv6,MLD,Redirect,
  - Snoofing : NS/NA,RS/RA,DHCPv6,Redirect,

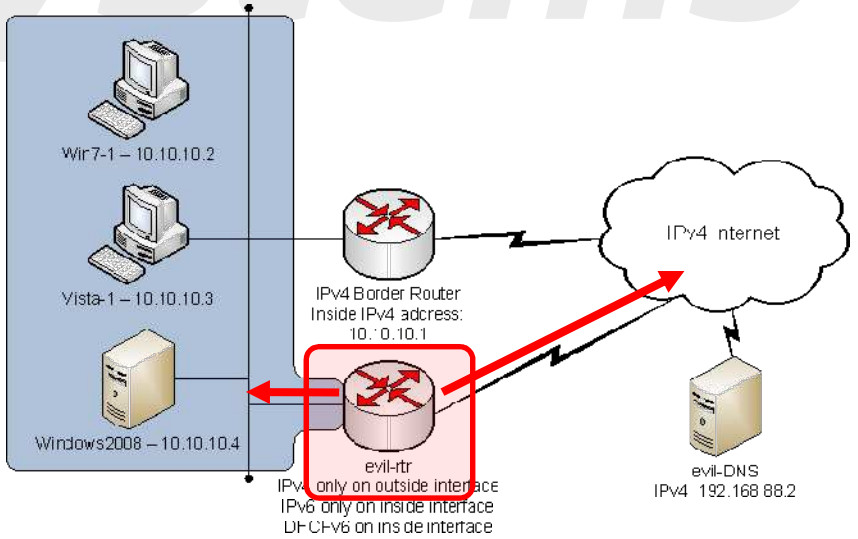
脅威の例1：SLAAC攻撃

概要

- 自動アドレス設定機構であるSLAACを悪用し攻撃
- 攻撃者は2つのインターフェースを持つホストを用意し、一方を社内へ接続し、もう一方はIPv4ネットワークに接続。この時、攻撃者はIPv4ネットワークに送信できるようにNAT-PTを実装
- 攻撃者は社内にRAを送出することで他のホストと接続可能となり、次にDHCPv6でDNSサーバ情報を提供し準備完了
- これにより社内のホストからの通信を攻撃者が通信を盗み取ることが可能となる

対応策

- IPv6を使用しないならIPv6機能をオフ
- 全てのデバイスでIPv6を無効化
- スイッチでプロトコル86DD(フレーム･タイプ)をブロック
- ルータでIPv6(プロトコル番号41)をブロックしロギング
- SeND(RFC 3971)/CGA(RFC 3972)のサポート
- スイッチでRA Guardを使う
- など



出典 http://resources.infosecinstitute.com/slaac-attack/

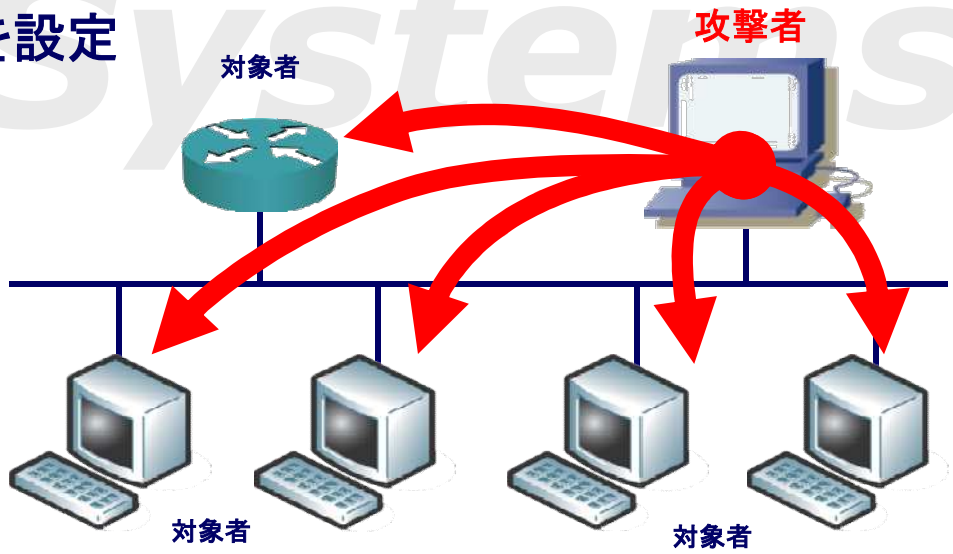
脅威の例2：大量のアドレス送信(DoS)

概要

- 異なるアドレスを大量に送出
- ネットワーク、キャッシュなどのリソース消費による通信不良、通信断、サービス停止、
- OSによっては再起動などになるものもあり

対応策

- 各種機器でNDPなどの上限値を設定



IPv6導入前の対策検討/実施　例1

課題

- 知らぬ間にトンネル接続などによりポリシーでは許可していないWebサイト、アプリケーションでの接続がされてしまうことがある

対策

- IPv6パケット、関連パケット(トンネル)を制御
- スイッチはフレームタイプ(IPv6は86DD)で制御
- ルータ、ファイアウォールはプロトコルタイプ、ポート番号の組合せなどで制御

関係するプロトコル・タイプ、ポート番号

- 41 : IPv6(ISATAP,6to4は41を使用)
- 43 : IPv6-Route Routing Header
- 44 : IPv6-Flag Fragment Header
- 58 : IPv6-ICMP ICMPv6
- 59 : IPv6 NoNxtNo Next Header
- 60 : IPv6-Opts Destination Options
- 3544 : UDP Teredo Default Port Number 3544　*:17 : UDP

```
Description SAMPLE CONFIG
  deny 41 any any
  deny 43 any any
  deny 44 any any
  deny 58 any any
  deny 59 any any
  deny 60 any any
  deny udp any any eq 3544
  deny udp any eq 3544 any
```

IPv6導入前の対策検討/実施　例2

課題

- Window 7など標準でIPv6 Enableになっているクライアントなどが想定外な時にIPv6、トンネルによって接続される

対応策

- コンロトールパネル -> ネットワーク接続のプロパティ -> ローカルエリア接続のプロパティの「インターネットプロトコルバージョン6」のチェックを外す
- トンネルはnetshコマンドでdisableに

netshコマンド　*:Windows 7の場合

- 6to4　: netsh interface 6to4 set disabled
  netsh interface 6to4 set state state=disabled undoonstop=disabled
- ISATAP : netsh interface isatap set disabled
  netsh interface isatap set state state=disabled
- Teredo : netsh interface teredo set disabled
  netsh interface teredo set state type=disabled

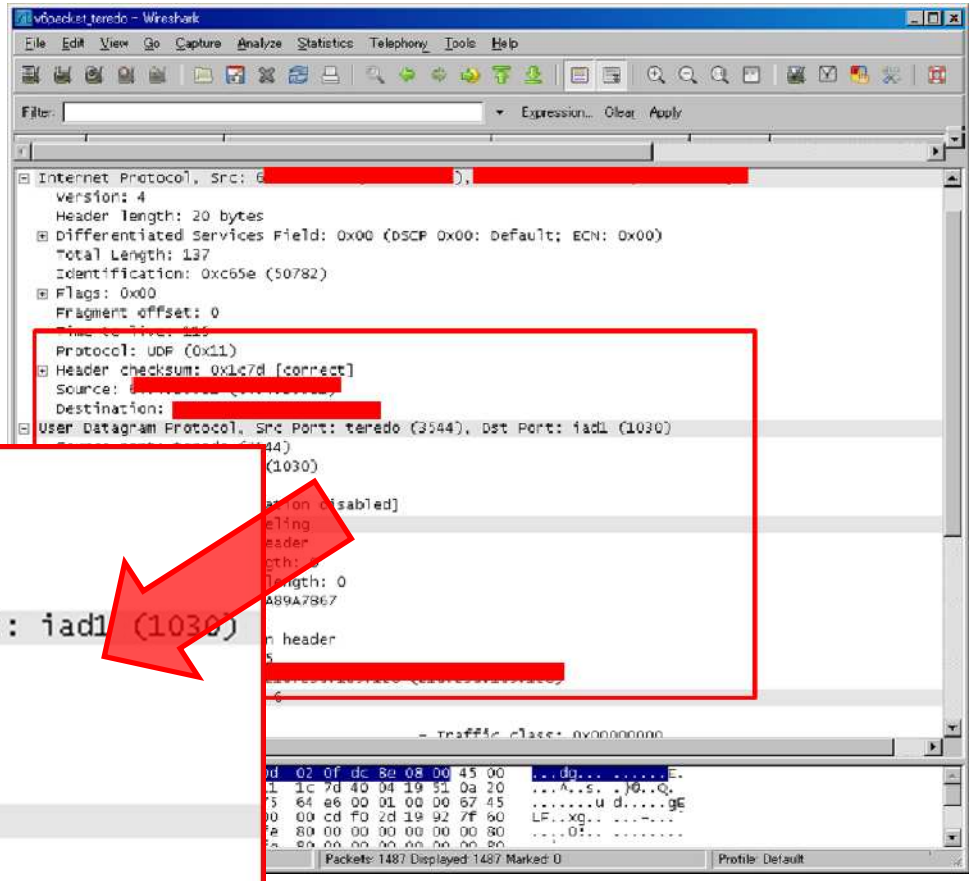
*:Teredo の接続サーバ、ポート番号などの変更

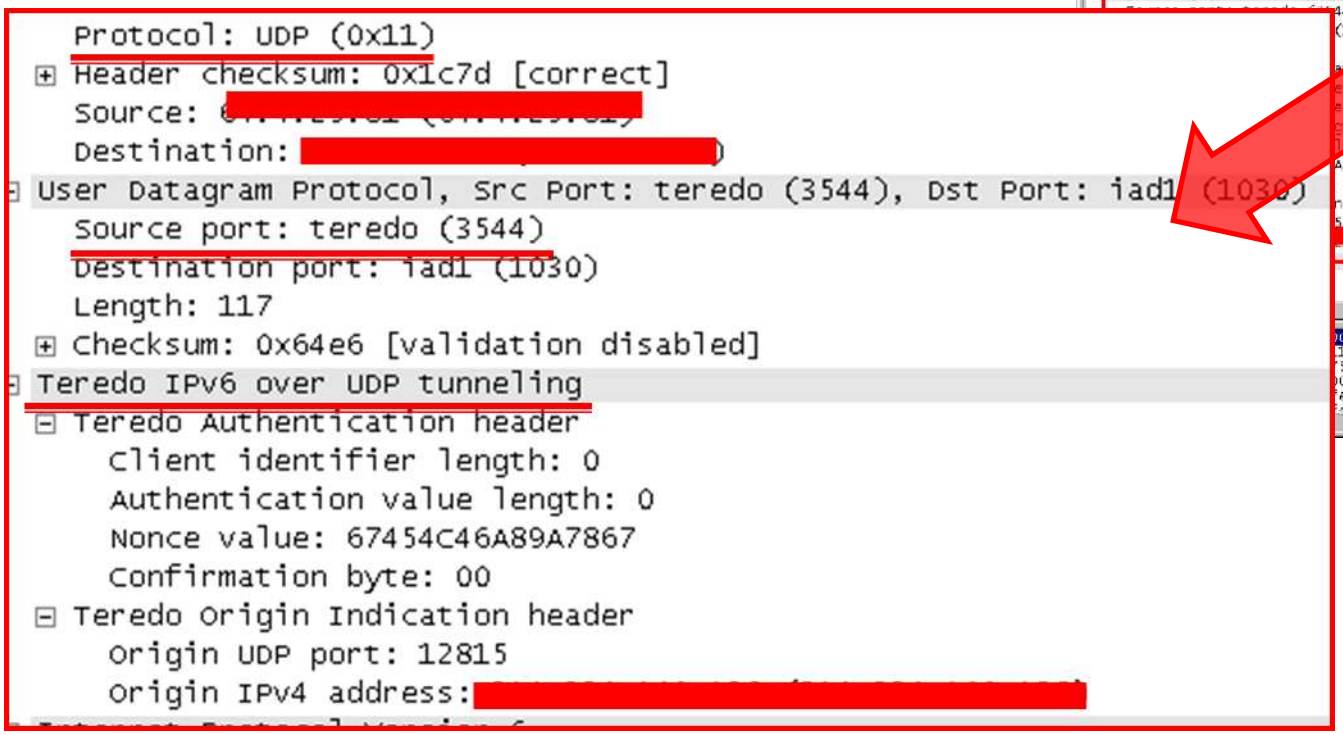
netsh interface teredo set state client **teredo.microsoft.com** **60** **34567**

サーバ名　接続間隔　ポート番号

Teredo のパケットキャプチャ

- 制御は製品によってはプロトコル・タイプ、ポート番号の組合せ、それ以外の指定もあるため注意が必要





Neighbor Discovery Protocol

- Neighbor Discovery Protocol
  - RFC4861（Neighbor Discovery for IP Version 6）
  - RFC4862（IPv6 Stateless Address Autoconfiguration）
- 主な機能をICMPv6で提供
  - IPv6アドレス解決（ARPの置き換え）
  - 重複アドレス検出（DAD）リダイレクション
  - 近隣ノードへの到達性のチェック
  - リンク上に存在する近隣ノードのMAC アドレスの判別
  - アドレスの変更・停止検出
  - リンク上にいるルータの検出及びパケットの転送先としての設定
  - ルータ探索アドレスの自動設定（SLAAC）
- 様々な重要な機能を提供していることからNDP、特にICMPv6は注意が必要

ICPMに関するポリシー

- IPv4/IPv6ではICMPの用途が異なる
- ファイアウォールなどICMPポリシーは変更しなければならない

ICMP Message Type	ICMPv4	ICMPv6
接続性確認	×	×
情報・エラーメッセージ	×	×
フラグメント通知	×	×
アドレス割り当て		×
アドレス解決		×
ルータ探索		×
マルチキャストグループ管理		×
モバイルIPv6		×

Neighbor Discoveryの課題 -1

- ルータ探索における攻撃
  - 攻撃対象のノードに対して攻撃者がデフォルトルータであるように振舞う
  - Router Advertisement（RA）をスプーフィングする
  - 意図的でなくても発生する可能性が最も高い
- アドレス設定における攻撃
  - 攻撃者が偽のPrefixを持ったRAを流し、攻撃対象ノードのアドレスを設定させる
  - アクセスルータのイングレスフィルタで偽プレフィックスを送信元にした通信をフィルタ
  - 偽プレフィックスを持ったホストにはルータを超えて到達できなくなる
  - さらに多くのプレフィックスを設定させることで攻撃対象ホストのサービス停止も可能
- アドレス解決における攻撃
  - 攻撃者は攻撃対象者のIPアドレスを名乗り上げることができる

Neighbor Discoveryの課題 -2

- 重複アドレス検出（DAD）における攻撃
  - 攻撃者は攻撃対象者のDADを妨害できる
  - 攻撃対象者はDADが完了できないためIPアドレスを設定できず、通信ができなくなる
- リダイレクトにおける攻撃
  - 攻撃者は自身がデフォルトルータであることをRAでリンクに通知する
  - 偽のデフォルトルータのRAを受け取った攻撃対象者の通信をリダイレクトする

    *:無効なホストに送ればDoS攻撃となり、有効なホストに送ればMITM攻撃となる

    ※ MITM攻撃 ：通信している2者間に介在し、情報を窃取する行為　(MITM：man-in-the-middle attack)
    中間者攻撃、中間一致攻撃、バケツ・リレー攻撃などとも呼ばれる
- ネイバーキャッシュにおける攻撃
  - サブネットワーク上のホストに対してスキャン攻撃を行い、ルータにNDのエントリーを作成させてリソースを浪費させる

Neighbor Discoverの対策(防御)

- RA Gurad
  - IPv6 Router Advertisement Guard （RFC6105)の利用
  - レイヤ2スイッチで、ルータ接続ポート以外からのルータ広告(RA)をフィルタリング
- Secure Neighbor Discovery (SeND)
  - CGA(Cryptographically Generated Addresses)を用いて IPv6の近隣検索の様々な機能を安全に実装するための仕組み
  - CGAを利用して、パケットの妥当性を検証する
  - SeND = NDP + crypto
    - Ciscoは実装済み　*:ソフトウエアVerによる
    - Linux、FreeBSDは対応
    - Windows Vista/7では未サポート
- その他
  - Private VLAN、Port securityはIPv6でも有効
  - 802.1xや802.1aeはIPv6でも有効
  - ブロードバンドアクセスで使われるDHCP-PD はNDP-proxyは必要ない　*

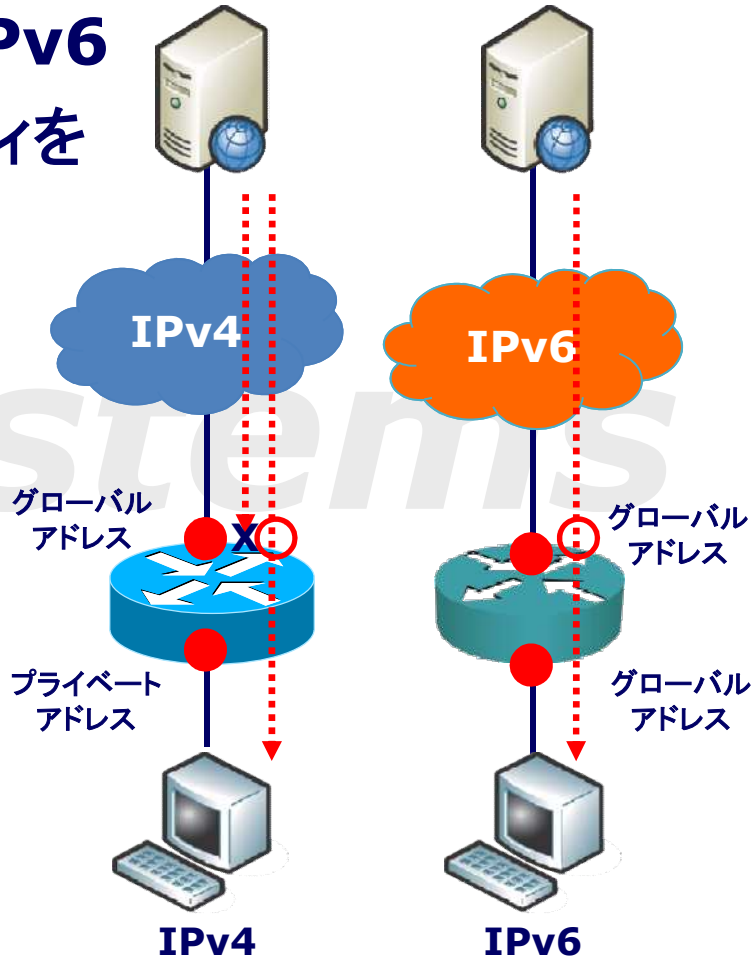
ICPMv6

Type	Name	Reference
0	Reserved	
1	**Destination Unreachable**	**[RFC4443]**
2	**Packet Too Big**	**[RFC4443]**
3	**Time Exceeded**	**[RFC4443]**
4	**Parameter Problem**	**[RFC4443]**
100	Private experimentation	[RFC4443]
101	Private experimentation	[RFC4443]
102-126	Unassigned	
127	Reserved for expansion of ICMPv6 error messages	[RFC4443]
128	**Echo Request**	**[RFC4443]**
129	**Echo Reply**	**[RFC4443]**
130	**Multicast Listener Query**	**[RFC2710]**
131	**Multicast Listener Report**	**[RFC2710]**
132	**Multicast Listener Done**	**[RFC2710]**
133	**Router Solicitation**	**[RFC4861]**
134	**Router Advertisement**	**[RFC4861]**
135	**Neighbor Solicitation**	**[RFC4861]**
136	**Neighbor Advertisement**	**[RFC4861]**
137	**Redirect Message**	**[RFC4861]**
138	**Router Renumbering**	**[Crawford]**
140	ICMP Node Information Response	[RFC4620]
141	**Inverse Neighbor Discovery Solicitation Message**	**[RFC3122]**
142	**Inverse Neighbor Discovery Advertisement Message**	**[RFC3122]**
143	Version 2 Multicast Listener Report	[RFC3810]
144	Home Agent Address Discovery Request Message	[RFC6275]
145	Home Agent Address Discovery Reply Message	[RFC6275]
146	Mobile Prefix Solicitation	[RFC6275]
147	Mobile Prefix Advertisement	[RFC6275]
148	Certification Path Solicitation Message	[RFC3971]
149	Certification Path Advertisement Message	[RFC3971]
150	ICMP messages utilized by experimental mobility protocols such as Seamoby	[RFC4065]
151	Multicast Router Advertisement	[RFC4286]
152	Multicast Router Solicitation	[RFC4286]
153	Multicast Router Termination	[RFC4286]
154	FMIPv6 Messages	[RFC5568]
155	RPL Control Message	[RFC-ietf-roll-rpl-19.txt]
156-199	Unassigned	
200	Private experimentation	[RFC4443]
201	Private experimentation	[RFC4443]
255	Reserved for expansion of ICMPv6 informational messages	[RFC4443]

出典 http://www.iana.org/assignments/icmpv6-parameters

IPv6におけるローカルネットワークの保護

- RFC4864 (2007年5月)
- Local Network Protection for IPv6
- 適切なパケットフィルタリングでセキュリティを確保
  - IPv6ローカルネットワークの保護のために達成すべき項目と方法
  - IPv4プライベート + NATと比較
  - IPv6では原則、NATなしで同様の保護を達成できると結論



Filtering ICMPv6 Message in Firewall

- RFC4890 (2007年5月)
- ファイアウォールにおけるICMPv6（Internet Control Message Protocol version 6）メッセージフィルタリング用の推奨仕様がまとめられた標準
- 実験の目的で使用されている ICMPv6や、定義されていないタイプの ICMPv6などがフィルタリングの対象
- エラー/インフォメーションメッセージなどの通過、中継などが記載されている

```
ipv6 access-list RFC4890 SAMPLE
    permit icmp any any echo-reply
    permit icmp any any echo-request
    permit icmp any any 1 3
    permit icmp any any 1 4
    permit icmp any any packet-too-big
    permit icmp any any time-exceeded
    permit icmp any any parameter-problem
    permit icmp any any mld-query
    permit icmp any any mld-reduction
    permit icmp any any mld-report
    permit icmp any any nd-na
    permit icmp any any nd-ns
    permit icmp any any router-solicitation
```

IPv6 Extension Header Filtering

- 必要に応じて拡張ヘッダのフィルタリングを検討
- 不用意にフィルタすると通信不能になることもあるので実施の際は注意が必要

Header Type	Next Header Code
Basic IPv6 Header	-
Hop-by-Hop Options	0
Destination Options (with Routing Options)	60
Routing Header	43
Fragment Header	44
Authentication Header	51
Encapsulation Security Payload Header	50
Destination Options	60
Mobility Header	135
TCP upper-layer	6
UDP upper-layer	17
ICMPv6	58
No Next Header Present	59

不正ルータ広告(不正RA) -1

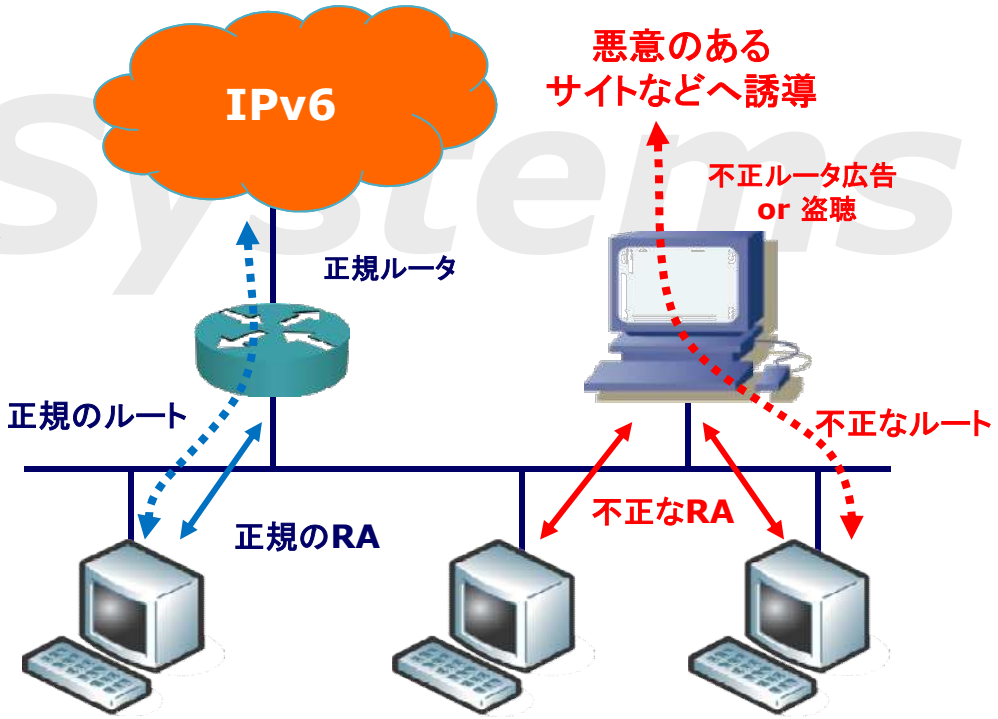
不正ルータ広告とは

- ルータ広告(RA)を送出すべきルータからの送信ではなく、他のルータなどから送出されるルータ広告を受信することで、意図しないアドレス/デフォルトが生成され通信不全になる

不正ルータ広告による影響

- 意図しないアドレス／デフォルト経路の生成
- 1つのパケットでセグメント内全体に影響を与える
- DHCPと異なりアドレスの追加設定が可能
- IPv4でも同様のことは発生する

*:DHCPv4



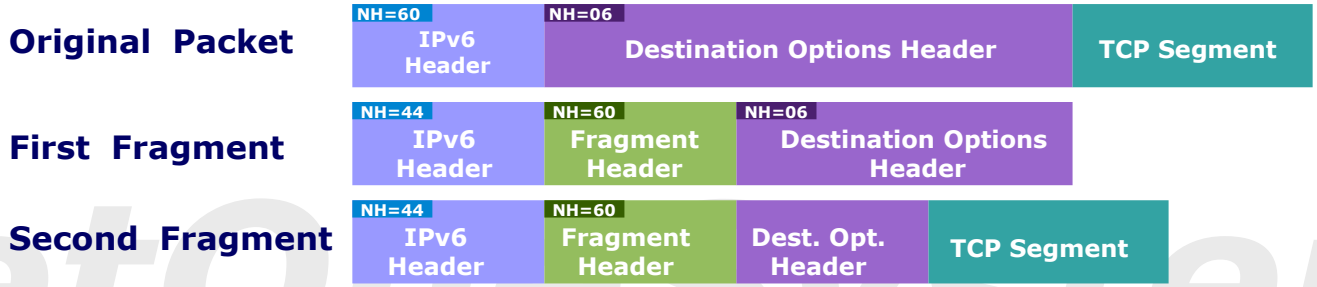
不正ルータ広告(不正RA) -2

対処･対策手法

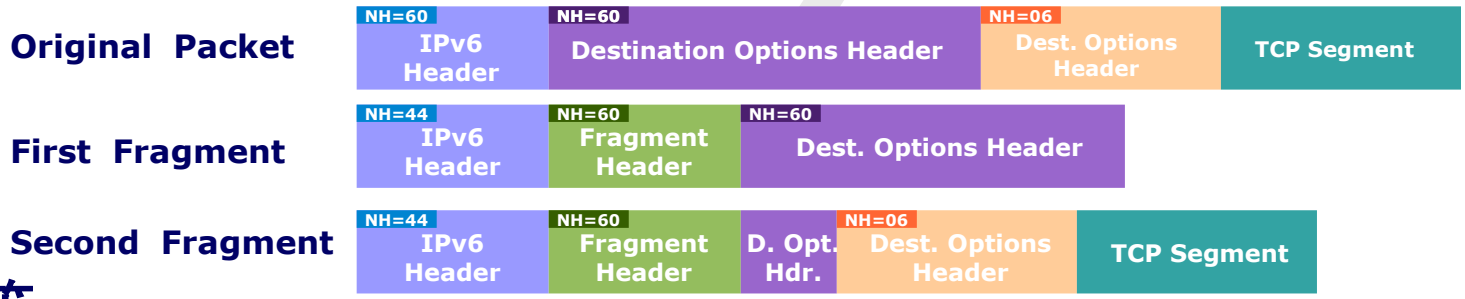
- RAを停止し、手動でアドレス、デフォルトルータなどの情報を設定
  - GUI、netshコマンドで設定
  - 手動入力による入力ミスなどに注意が必要
- RA Gurad
  - IPv6 Router Advertisement Guard （RFC6105)の利用
  - L2スイッチなどで指定されたRA以外をフィルタリングする機能
- モニタリングによる対策
  - NDPMon： セグメント内の NDP パケットの異常を検知
  - rafixd(KAME)： 不正 RA と同じ RA を Router Lifetime=0 で広告、不正 RA による機器内容をリセット
  - ramond :不正 RA と同じ RA を Router Lifetime=0 で広告、不正 RA による機器内容をリセット
- SeND(Secure Neighbor Discovery)の導入
  - SEcure Neighbor Discovery （RFC3971)の利用

RA Guradの回避手段が…

- スイッチなどに実装している「RA Gurad」を回避する攻撃手段が2種類存在していることが判明
  - RAメッセージに拡張ヘッダを用いる



  - IPv6フラグメントを用いる

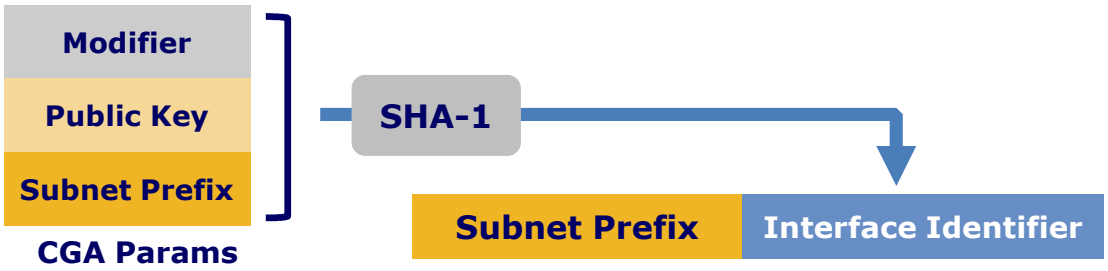


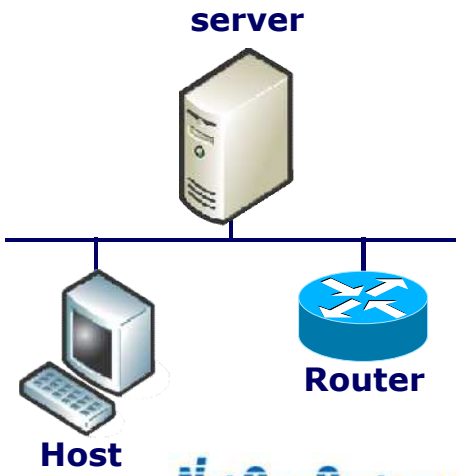
- 対応策
  - RAの識別にヘッダーチェーンを制限
  - 識別出来ない場合は、送信元アドレスがリンクローカル、または未指定(::)でブロック

出典 http://tools.ietf.org/html/draft-gont-v6ops-ra-guard-evasion-01

Secure Neighbor Discovery (SeND)

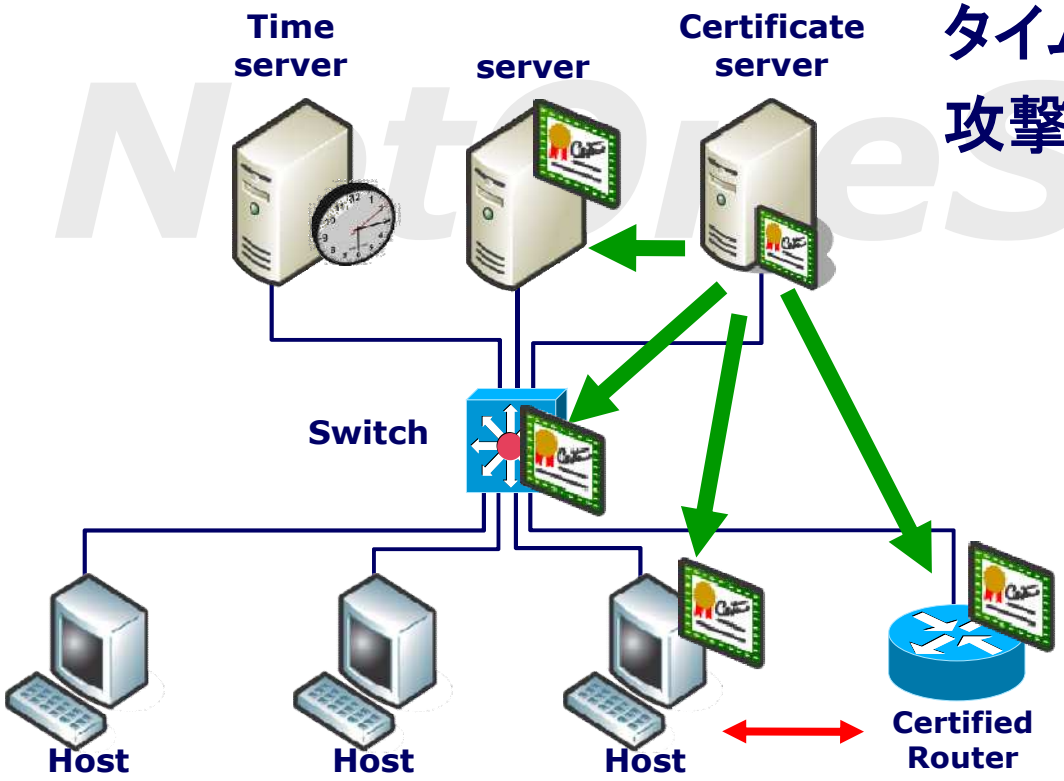
- RFC3971 （2005年3月）
- CGA(Cryptographically Generated Addresses)を用いてIPv6の近隣検索の様々な機能を安全に実装するための仕組み
- ホスト間の公開鍵とそれを使用して生成されたIPv6アドレス、そしてRSA電子署名を使用してパケットを送受信することで、パケットの改竄検出やアドレス詐称を防止
- アドレスの所有、NDPのメッセージ、Default Routerの正当性を担保

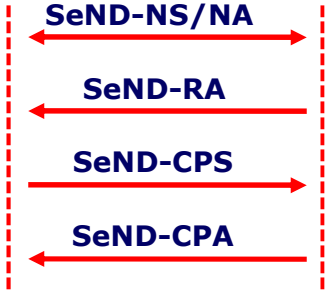




Secure Neighbor Discovery (SeND)

- 利点として、PKIのような認証基盤を必要としない
- 誰でも公開鍵と秘密鍵のペアを作れることから送信者からのパケットであることを検証
- 同時に、電子証明書を使用してルータとの信頼関係の構築やタイムスタンプを使用してリプレイ攻撃の防止策としても利用可能





CPS : Certification Path Solicitation
CPA : Certification Path Answer

SeND利用時の注意

- SeNDは広く普及している技術ではない
  - 一つのルーターだけがSeNDをサポートしていても、利用者が操作するパソコンやサーバーがSeNDのパケットを生成したり、検証できなければ、その効果はない
  - ネットワーク内のすべてのノードがサポートできてこそ効果がある
- 秘密鍵・公開鍵のペアを全ての機器に設定する必要がある
- IPアドレスにハッシュを埋め込むことから必ずしも暗号強度が高いとは言い切れない
- オーバーヘッドが増加
  - ルータは頻繁にキー計算が行われる（前もって行う場合もあり）
  - ルータはより多くのステート情報を保持する必要
- DoS攻撃のターゲットになる可能性もある
- 実装
  - FreeBSD、Linux、Cisco IOS ※Microsoft: Windows Vista/7/2008では未サポート

IAB Thoughts on IPv6 Network Address Translation

RFC5902 (2010年7月)

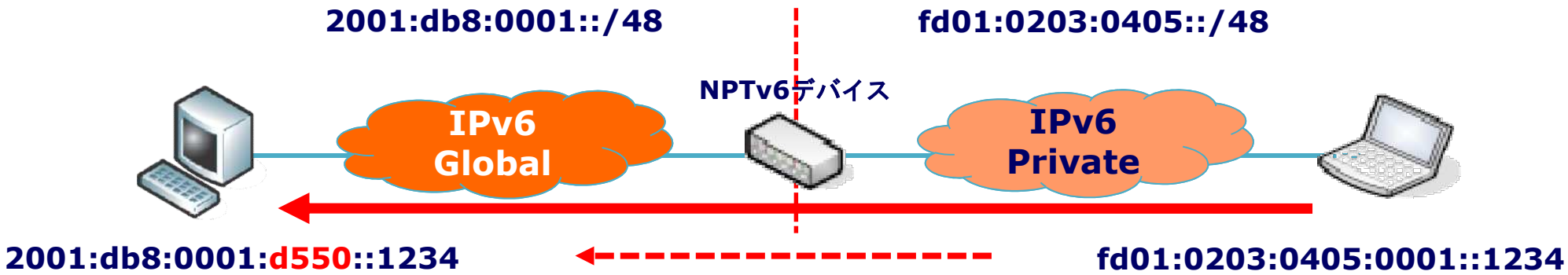
- IPv6ローカルネットワークの保護(RFC4862)の為の項目として IPv4+NATと対比し議論した結果、IPv6おいてNATなしで保護が可能と結論ずけされた
- が、その後もNATの議論が繰り返された為、
- IABが「End-to-Endの原則」に照らしてNATおよびIPv6の関係を整理
- NATの有効性を考えるのではなく、NATを利用することでインターネットへの影響が受けるかを考慮
- 結論として次の可能性を考慮
  - アドレス変更(アドレスリナンバリング)
  - マルチホーム対応
  - 設定情報の統一

NAT44

- ネットワーク出入り口でのフィルタリング
- トポロジの隠蔽とプライバシ

IPv6-to-IPv6 Network Prefix Translation

- RFC6296（2011年6月）
- 当初はNAT66で提案、NPTv6 (IPv6-to-IPv6 Network Prefix Translation) に変更
- エンドエンドの通信を保つため1:1で変換し、ポートのマッピングは行われない
- 内部ネットワークで使われるユニーク・ローカルIPv6ユニキャスト・アドレス(RFC4193)のプレフィックスをそのままグローバルなIPv6プレフィックスと置き換える
- アドレス全体のチェックサム(RFC1071/RFC1624)が変わらない
- 注意として、サブネットに0xFFFFは利用できない



IPv6導入事例紹介

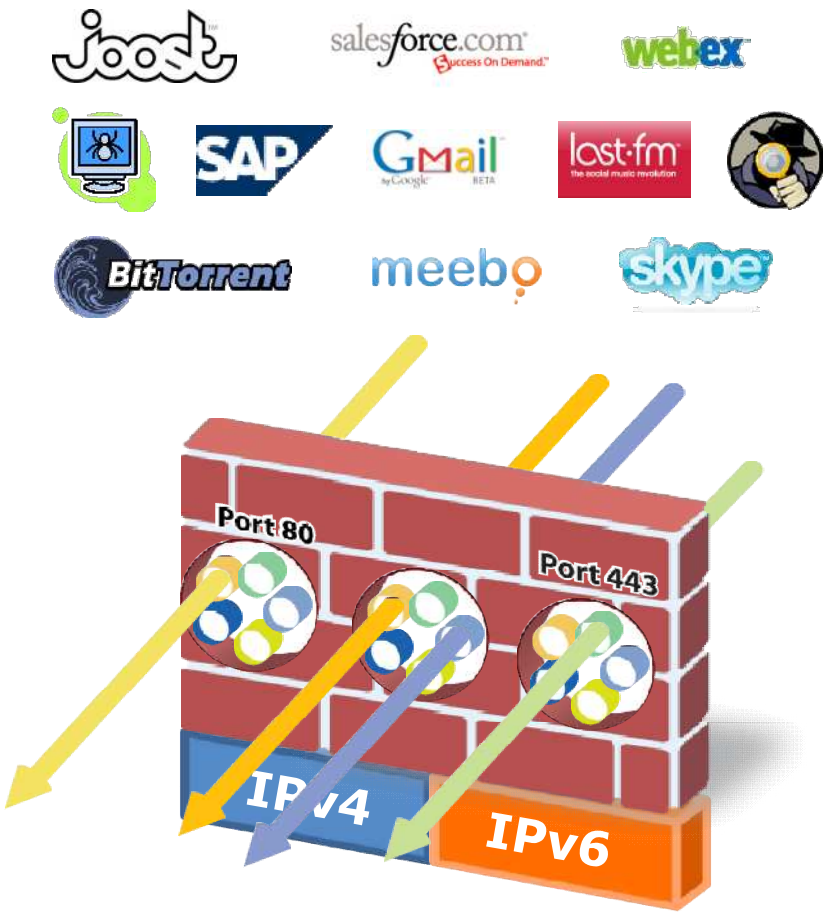
モチベーションとスケジュール

- モチベーション
  - システム/アドレス計画/設計変更
- スケジュール
  - 2007年：IPv4アドレス枯渇を意識しIPv6各種市場動向など調査検討開始
  - 2009年：自社IPv4アドレス設計変更などプラン
  - 2010年：IPv6テスト導入プラン検討開始
  - 2011年：パラレル･モデルで構築準備中

ファイアウォールの要件

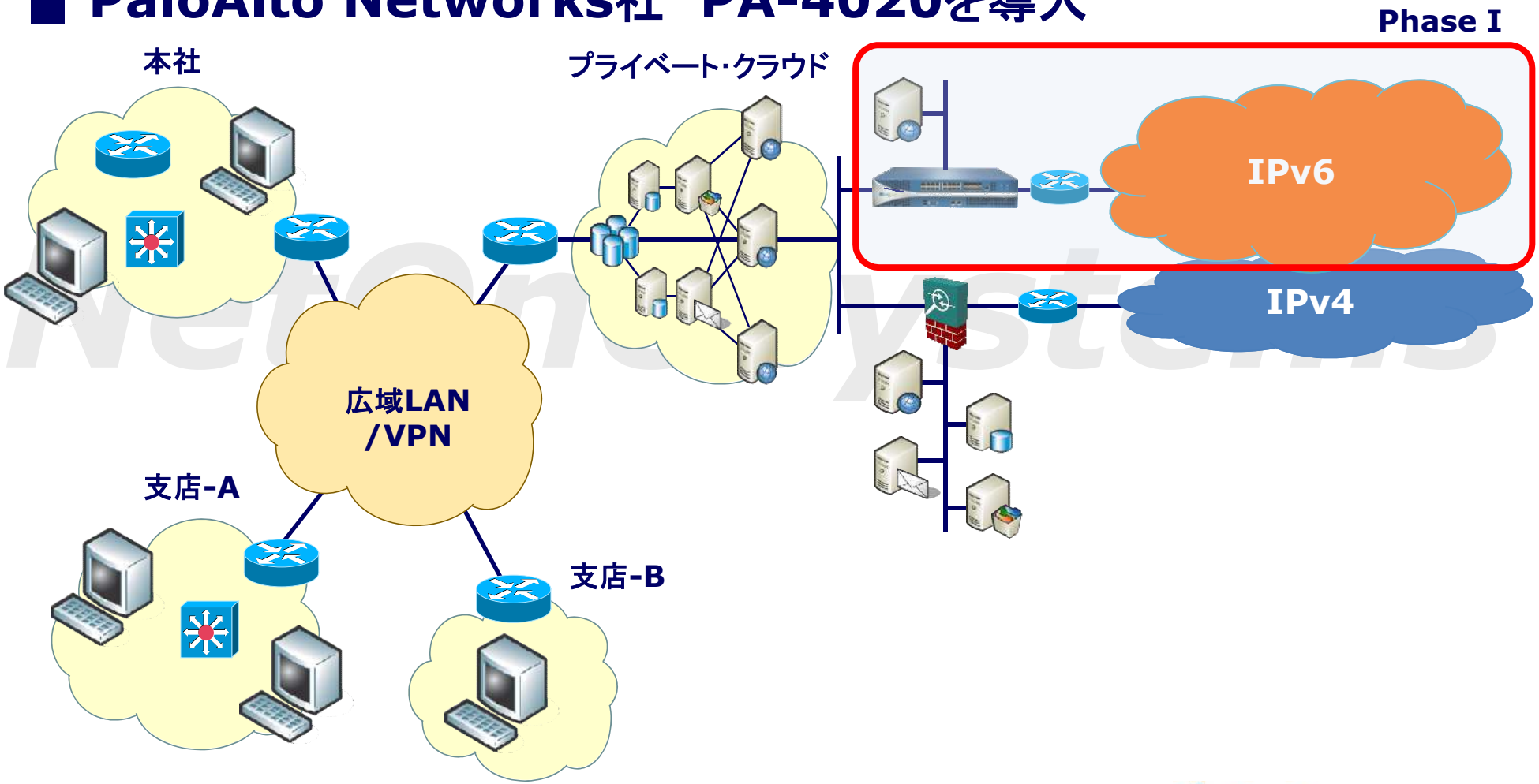
ファイアウォールに対する新しい要件

1. ポート番号、プロトコル、秘匿技術やSSL暗号に関わらずアプリケーションを識別
2. IPアドレスに関わらず利用ユーザーを識別
3. ユーザーのアプリケーション利用の可視化およびアクセス制御を実現
4. アプリケーションに埋もれて通過する脅威や重要データをリアルタイムでブロック
5. パフォーマンス劣化がないインライン導入を可能にするマルチギガビット処理
6. デュアルスタック化(IPv6の対応)



導入事例

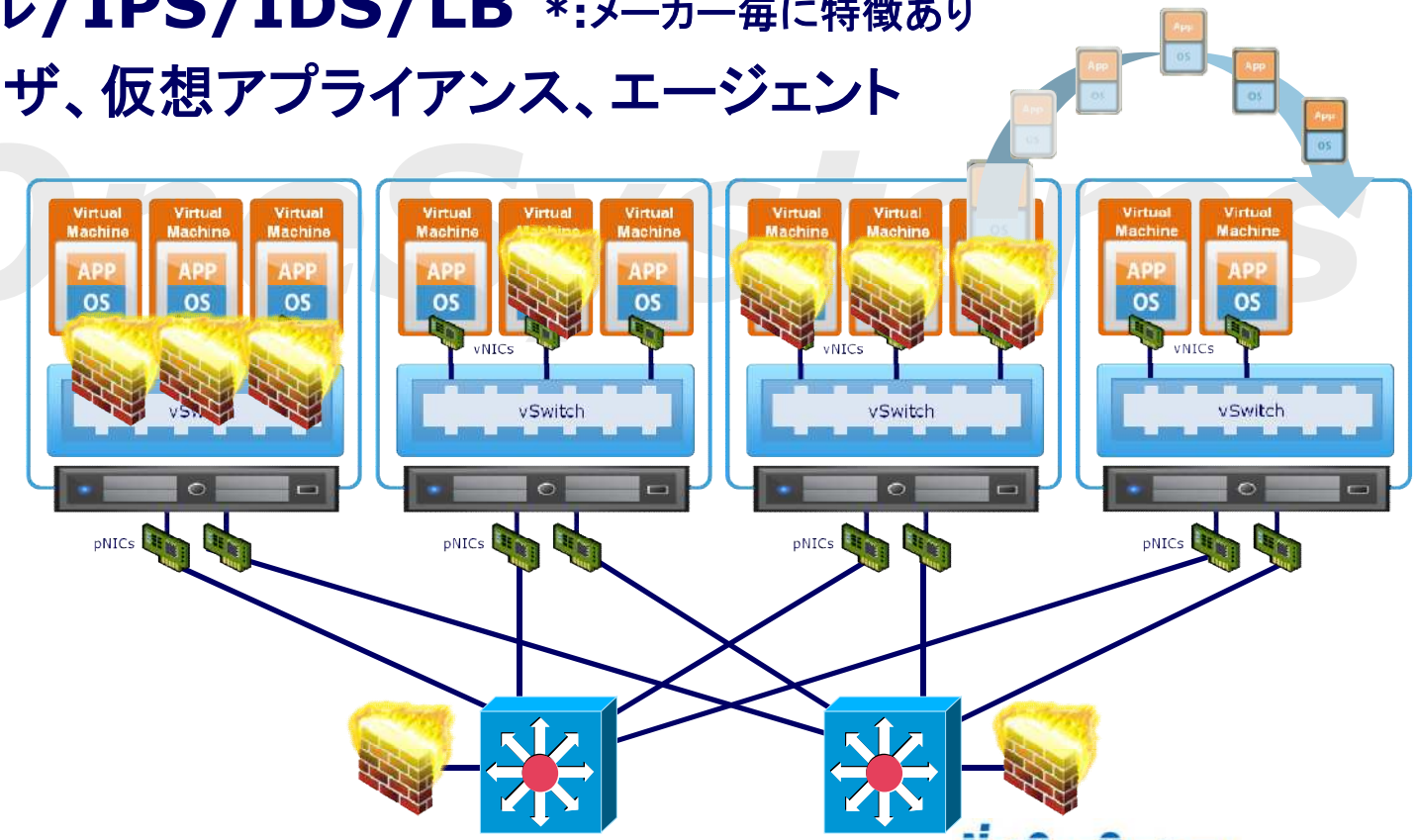
- パラレル・モデル
- PaloAlto Networks社　PA-4020を導入



仮想化時代のIPv6セキュリティ

仮想化時代のIPv6セキュリティ

- サーバ/ネットワークの仮想化が進展することでIPv6ネットワークと同時にセキュリティの考慮が必要
- IPアドレス、pNIC、vNIC、MACアドレス、VM間通信、etc、
- ファイアウォール/IPS/IDS/LB *:メーカー毎に特徴あり
  - ハイパーバイザ、仮想アプライアンス、エージェント



まとめ

まとめ

- セキュリティの課題はIPv4、IPv6共に大きな変化はない
- 知らない間にIPv6による脅威は始まっている
- 対応可能な範囲は早期に実施

- IPv6が導入されることで一時的に運用など含めた作業量が2倍以上になることも想定される
- 本格導入期を迎える前に、正しい知識と理解でIPv6による脅威の対策を
- これらの積み重ねが、企業ICTシステムのディペンダビリティ向上に繋がる
  - 信頼性（reliability）、保全性（maintainability）、可用性（availability）

- 今後の課題として、完全には表面化していない新たな脅威についても学ぶ必要がある

参照サイト

- IPv6 普及・高度化推進協議会
  - セキュリティ WG　IPv6 対応セキュリティガイドライン（第 0.5 版）
    http://www.v6pc.jp/jp/upload/pdf/swg-IPv6SecurityGuideline_0.5.pdf
  - IPv6導入に起因する問題検討SWG　IPv6導入時に注意すべき課題
    http://www.v6pc.jp/jp/upload/pdf/2011093001_v6fix.pdf
- 内閣官房情報セキュリティセンター
  - 政府機関の情報セキュリティ対策のための統一技術基準
    http://www.nisc.go.jp/active/general/pdf/K305-101.pdf
- 独立行政法人 情報処理推進機構 (IPA)
  - TCP/IPに係る既知の脆弱性に関する調査報告書 改訂第5版
    http://www.ipa.go.jp/security/vuln/documents/vuln_TCPIP.pdf
- 日本セキュリティオペレーション事業者協議会(ISOG-J)
  - IPv6検証報告書
    http://www.jnsa.org/isog-j/output/2011/ISOG-J_IPv6_Verification_Report.pdf
- シスコシステムズ合同会社
  - Implementing First Hop Security in IPv6
    http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- NIST
  - Guidelines for the Secure Deployment of IPv6
    http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf
- ICSAlabs
  - IPv6 Capable Security Products
    https://www.icsalabs.com/technology-program/ipv6/ipv6-capable-security-products

http://www.netone.co.jp