Internet Week 2009

点検! IPv6のセキュリティ
ープロトコル挙動の観点からー

アラクサラネットワークス(株) ネットワーク技術部
鈴木伸介 〈suz@alaxala.net〉

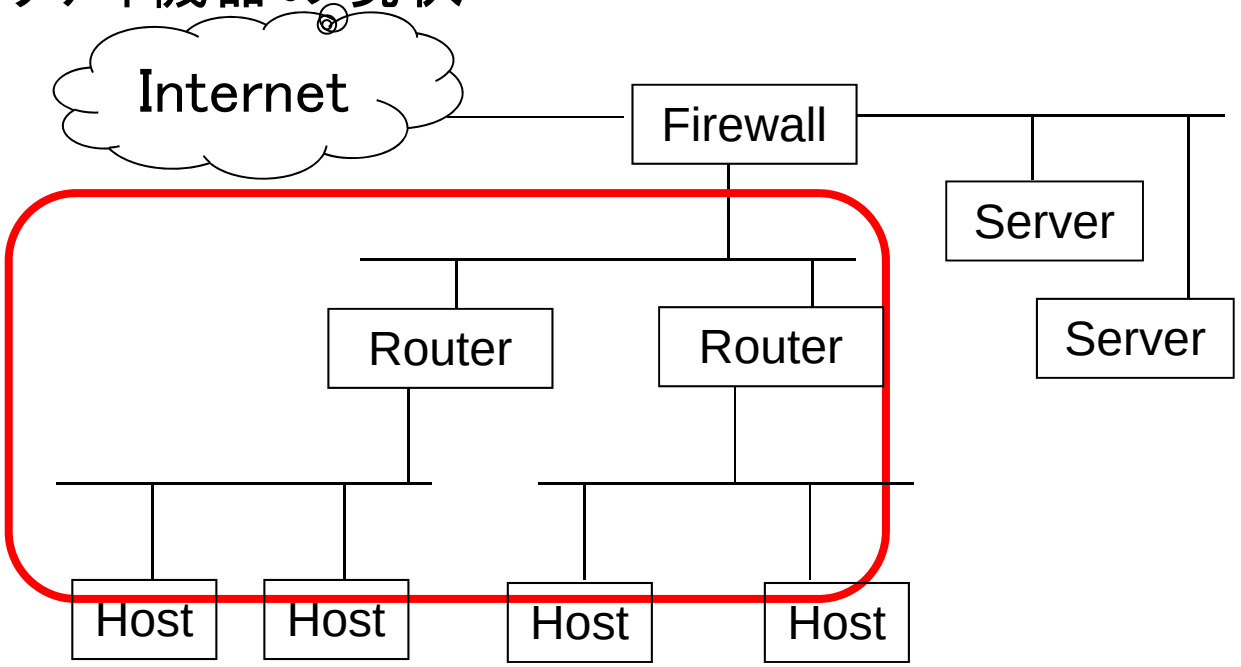
AlaxalA
For The Guaranteed Network

本発表の分析対象

端末収容LANのセキュリティ分析

下記は別発表にてカバーします

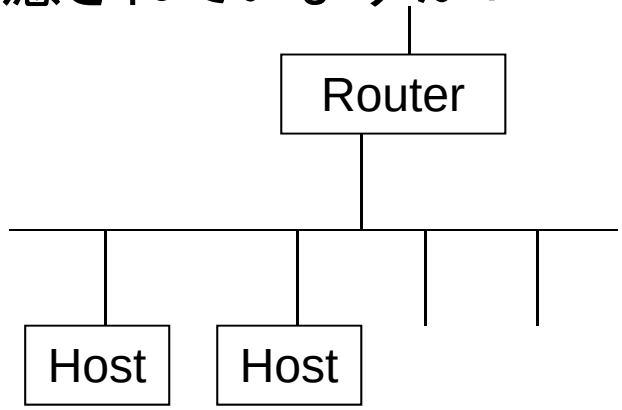
- インターネット側のセキュリティ分析
- サーバ・端末に特化したセキュリティ分析
- アプリケーション層のセキュリティ分析
- セキュリティ機器の現状



はじめに

IPv4では、どの位LAN上のセキュリティを考慮されていますか?

①意図せぬ端末をつながせないように工夫
　物理制御、プロトコル制御、法的制御、…
②何かあったときに追跡しやすいように工夫（性善説）
　MAC登録、IP登録、(MAC,IP)対応登録、…
③何かあったときに追跡しやすいように工夫（性悪説）
　IP詐称防止技術、端末監視ソフト導入、…
…



→IPv6でも基本的には同じレベルの対策が必要になるはず

ARP->NDP，DHCPv4->DHCPv6/RAとなるが、プロトコル挙動は基本的に同じ

本発表では、IPv6が網内に入ってくると発生する
忘れがちなポイント
すぐに取れそうな対策
を紹介します。

注意

①意図してIPv6を導入する場合と、気づかぬままIPv6が入る場合があります。
→特に後者に要注意。

例1. IPv6自動トンネルによるIPv6

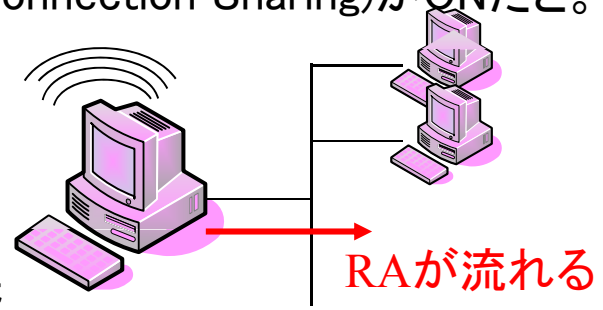
6to4 = IPv4グローバルアドレスがあれば、IPv6接続可能

Teredo = IPv4プライベートアドレスしかなくても、Teredoサーバ・リレーに到達できれば、IPv6接続可能

例2. Windowsで、ICS (Internet Connection Sharing)がONだと。。。

・無線LANを複数端末で共有

・6to4などでIPv6コネクティビティ確保



http://technet.microsoft.com/ja-jp/library/cc779985(WS.10).aspx

②「常に正しい答え」はありません。
「放置したことによる損害」と「 対策したことによる負担」のトレードオフ

※Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です

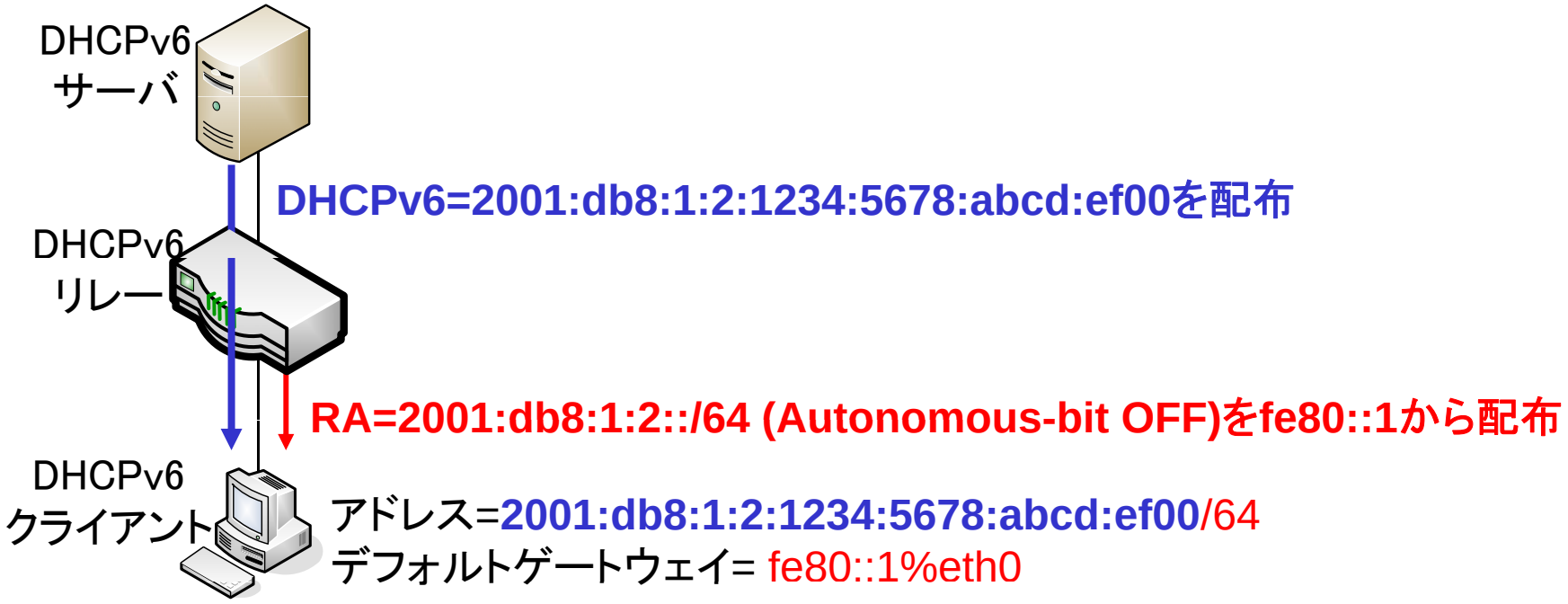
1. 意図せぬアドレス生成（RA）

（1） 背景

・IPv4アドレス生成＝DHCPv4

・IPv6アドレス生成＝事実上RAが必須

（DHCPv6ではデフォルトゲートウェイやPrefix長を配布できない）

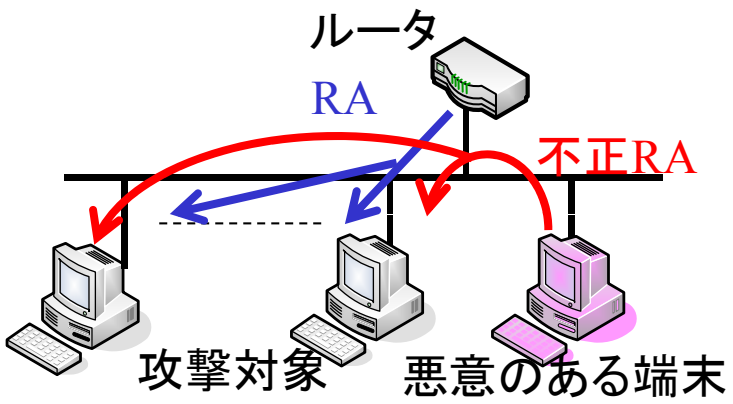


1. 意図せぬアドレス生成（RA）

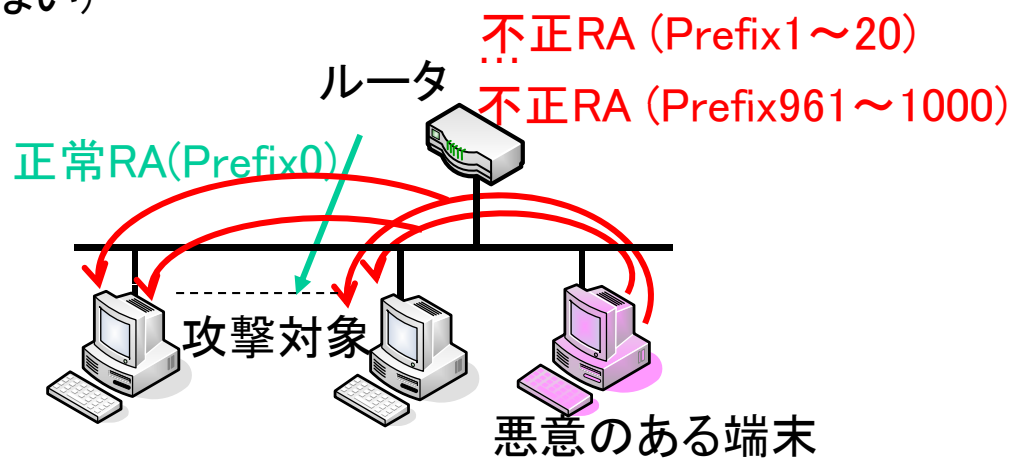
(2) RAを悪用した攻撃・脅威

・RAは、パケット1つ流すだけでセグメント内全体に波及

(※DHCPでは(事実上)unicastで端末−サーバ間のやりとりをするため、
そこまで大きく波及させることが出来ない)



デフォルトゲートウェイ=悪意のある端末



1001個のグローバルアドレスを生成

・想定される脅威 （偽DHCPv4サーバを設置されるリスクと同じ）
通信断、盗聴、端末のメモリ消費DoS、意図せぬIPv6通信

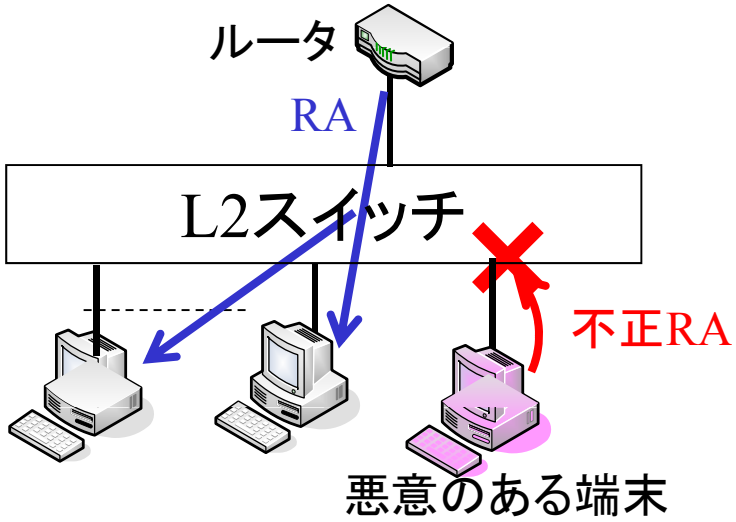
※気が付かぬままRAを流してしまっている端末も、意外と多いです

1. 意図せぬアドレス生成（RA）

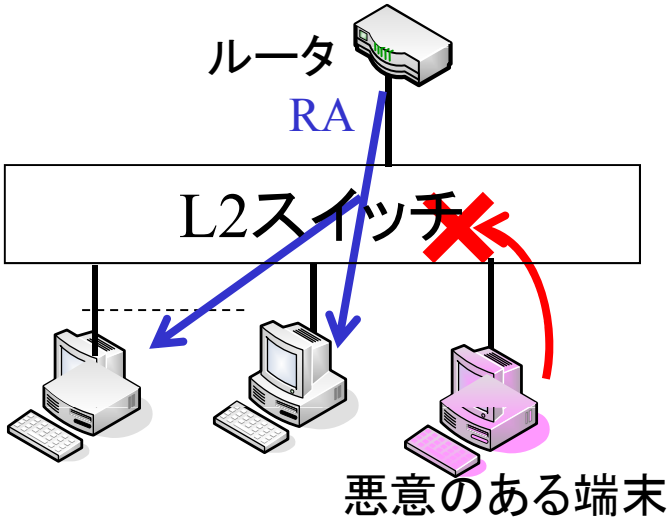
(3) 抜本対策

（標準化の場でも議論中ですが、ここでは「今できること」に絞ります）

「意図せぬRA」を流せなくすることが一番大事（実現方法はいろいろ）



端末収容ポートでRAをフィルタ廃棄



そもそも端末間通信を許容しない
(Private-VLAN, Privacy-Separation, …)

1. 意図せぬアドレス生成（RA）

(4) オペミスのみ対策

・「悪意のある端末からの攻撃はまずない」と仮定し、「オペミスでRAが流れるケース」への対応を重視するのも一案

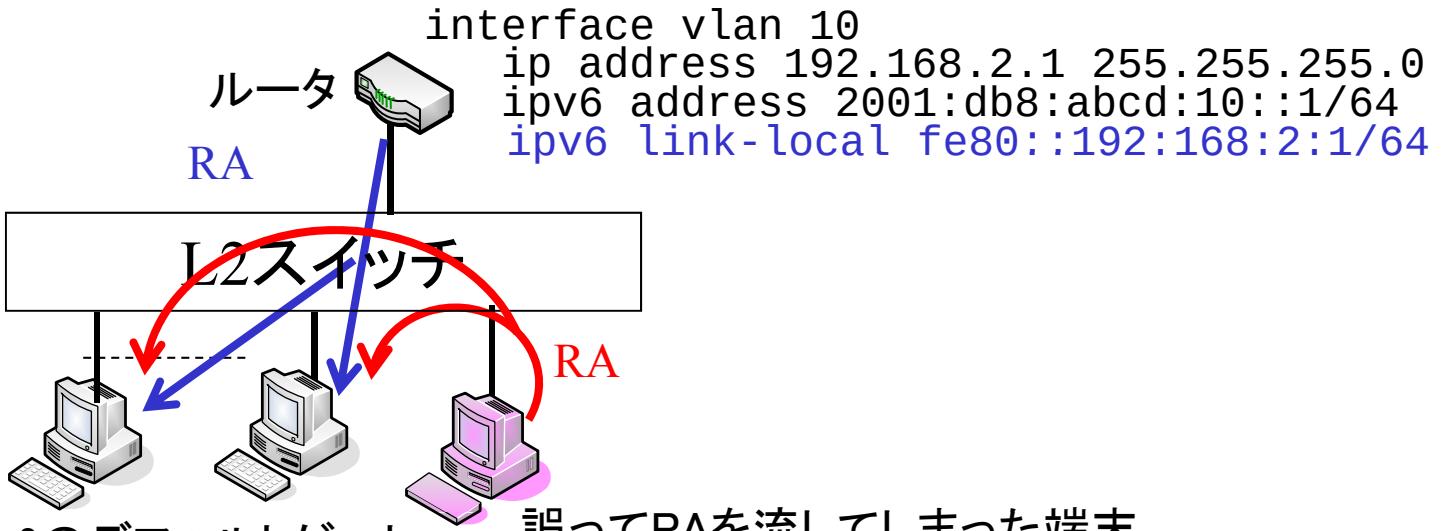
・対策案は数案あります。

1. ルータのリンクローカルアドレスを、手動設定
2. MACアドレスに注目して、意図せぬRAの発信元を追跡
3. 「意図せぬRAを打ち消すRA」を再送信
4. 本来のRAの優先度を高くする

1. 意図せぬアドレス生成（RA）

（4）オペミスのみ対策 （例1）

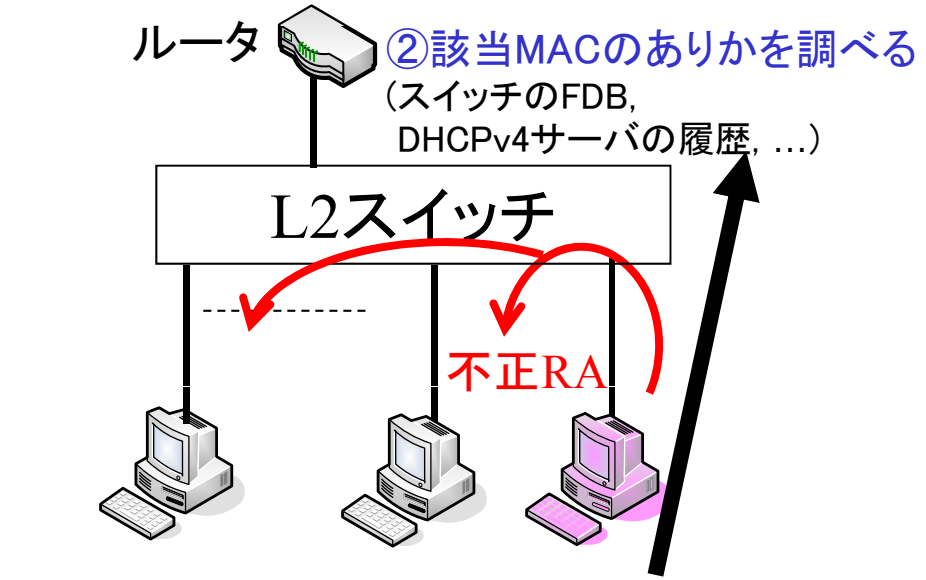
ルータのリンクローカルアドレスを、EUI64ではなく、わかりやすい値に手動設定
→ デフォルトゲートウェイのアドレスから、意図せぬRAを発見可能



1. 意図せぬアドレス生成（RA）

(4) オペミスのみ対策 （例2）

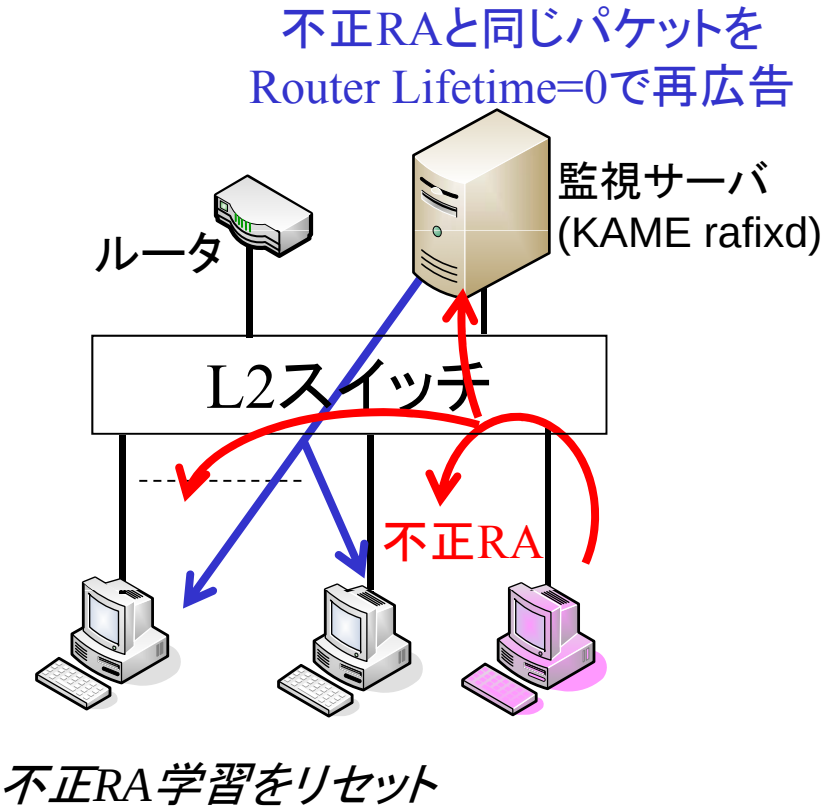
意図せぬRAのMACアドレスに注目して、RA発信元を追跡



1. 意図せぬアドレス生成（RA）

(4) オペミスのみ対策 （例3）

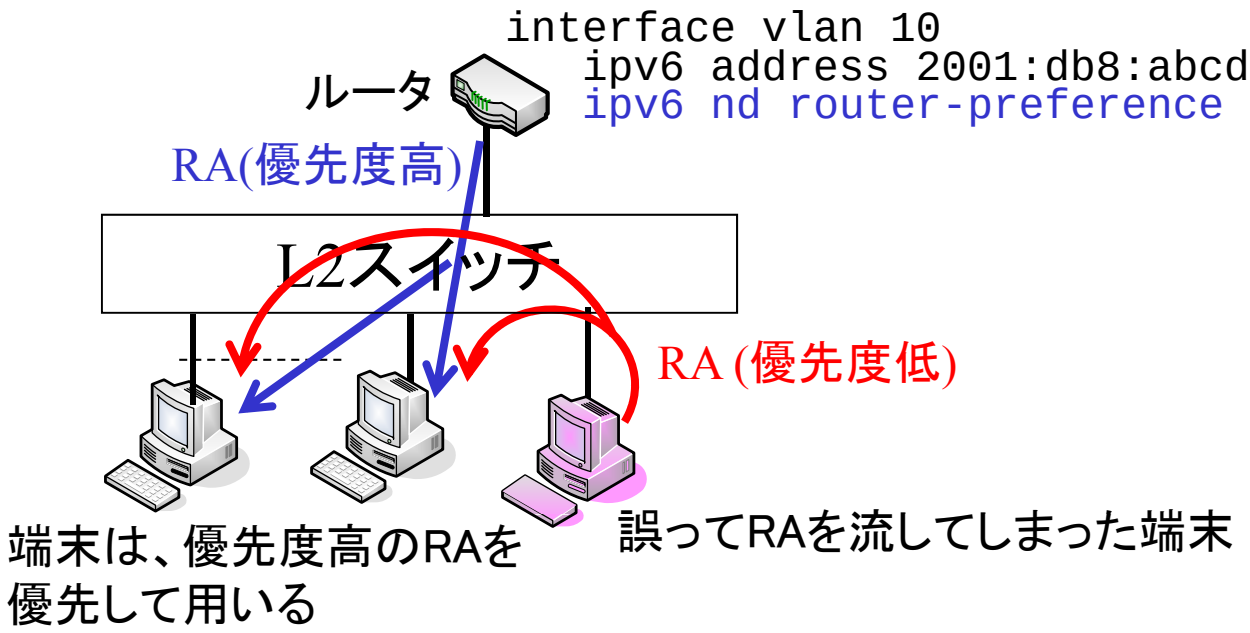
意図せぬRAをリセットするRAを出しなおす （KAME rafixd）



1. 意図せぬアドレス生成 (RA)

(4) オペミスのみ対策 （例4）

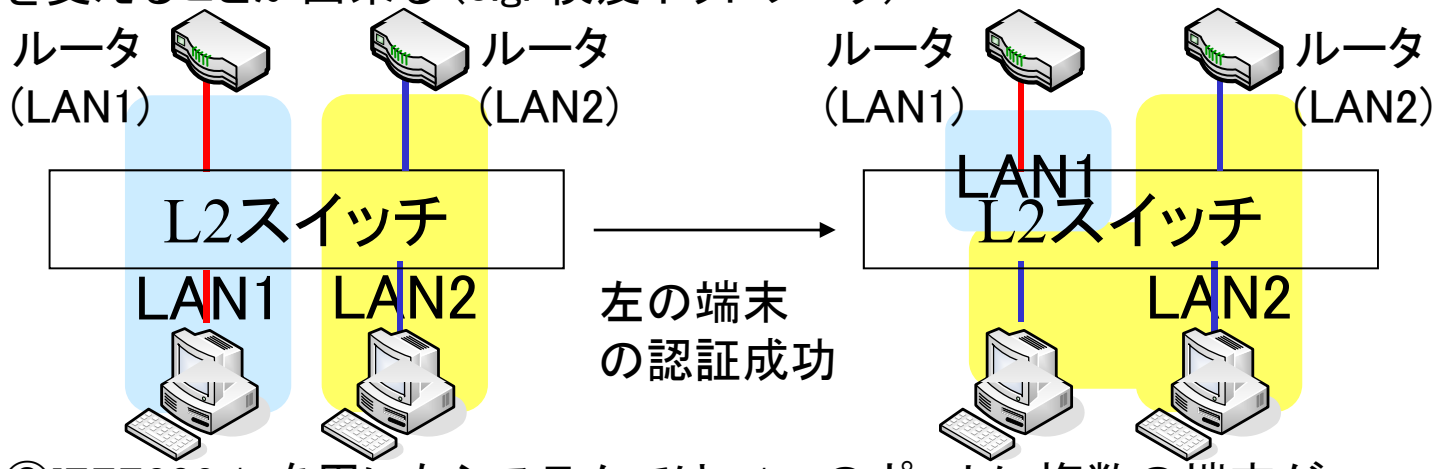
・本当のルータからのRAの優先度を高くする (Router Preference; RFC4191)



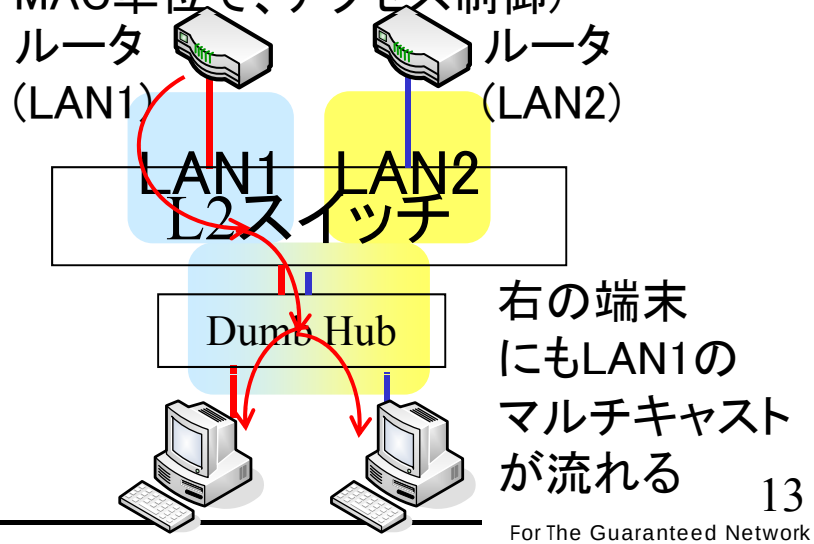
2. IEEE802.1x(無線)とIPv6の相性問題

(1) 背景

①IEEE802.1xでは、端末の認証結果によって、端末収容VLAN
を変えることが出来る (e.g. 検疫ネットワーク)



②IEEE802.1xを用いたシステムでは、1つのポートに複数の端末が
ぶら下がることもある (ポート単位ではなく、MAC単位で、アクセス制御)
(esp. 無線LAN)
→上流から流れたマルチキャスト
パケットは複数VLANに漏れる

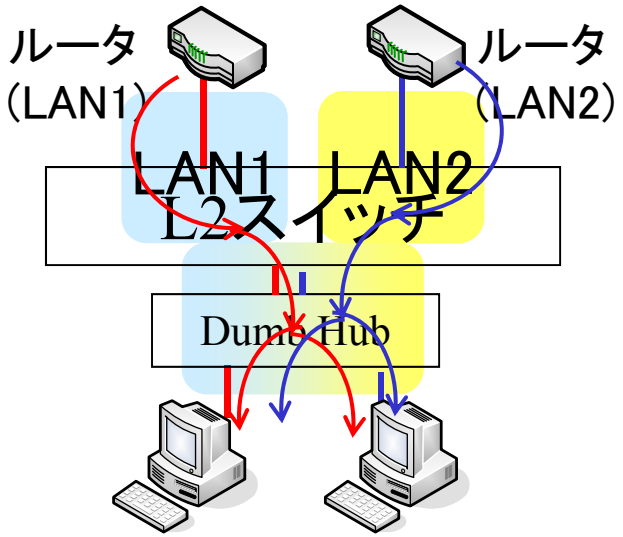


2. IEEE802.1x(無線)とIPv6の相性問題

(2) IEEE802.1x(無線)とIPv6の相性問題

IPv6アドレスは、IEEE802.1xの認証結果に関わらず、全てのVLANから手に入ってしまう（RAはマルチキャストでルータから流れるため）

※DHCPv4は実質ユニキャストでやりとりされるため、本件非該当



- 想定される脅威

意図せぬIPv6通信をトライすることによる、IPv6通信断

e.g.) LAN1の端末が、LAN2のルータ経由の通信を試みる

LAN1の端末が、LAN2のアドレスをソースにした通信を試みる

IEEE802.1xをIPv6環境では適用不可

2. IEEE802.1x(無線)とIPv6の相性問題

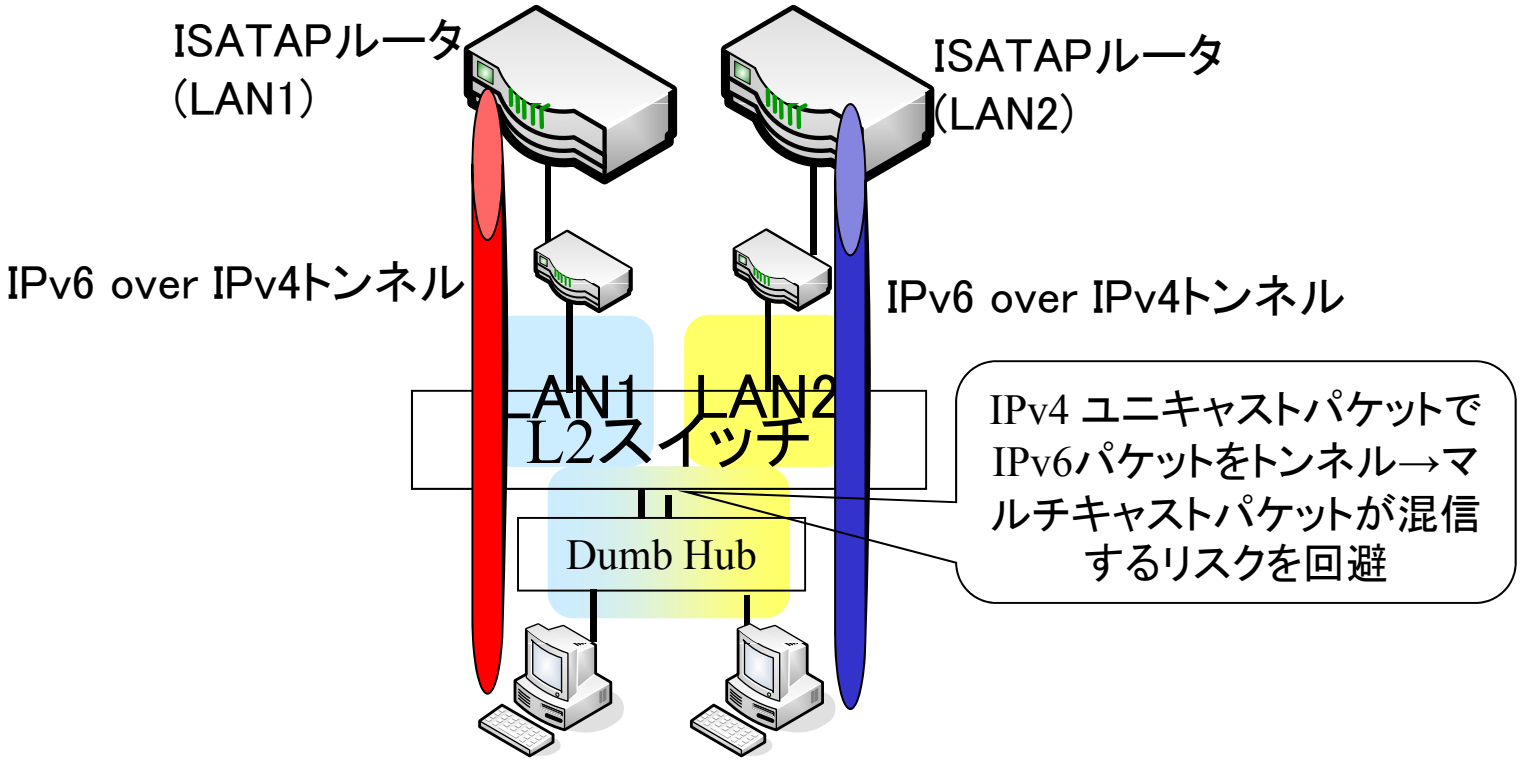
(3) 対策 (標準化の場でも議論中ですが、ここでは「今できること」に絞ります)

・IPv6 over IPv4トンネルによるIPv6接続

e.g.) ISATAP

※ISATAPルータ(通常はDNS hostnameで選択)を切り替える必要あり

・IEEE802.1xを用いる区間ではIPv4パケットしか流れないため、本問題に非該当



2. IEEE802.1x(無線)とIPv6の相性問題

(3) 対策 (cont.)

・混在しても困らないようなRA広告 + DHCPv6でのアドレス配布

①ルータのリンクローカルアドレスを全て同じにする

②RAのMACアドレス通知オプションをOFFにする

③RAで広告するPrefixは、自動設定の対象外とする

④RAで広告するPrefixは、Onlinkではないことにする

⑤ICMPv6 RedirectをOFFにする

```
interface vlan 10
   ipv6 address 2001:db8:abcd:10::1/64
 ①ipv6 address fe80::1 link-local
   ipv6 nd management-config-flag
 ②ipv6 nd no-advertise-link-address        ④           ③
   ipv6 nd prefix 2001:db8:abcd:10::/64 off-link no-autoconfig
 ⑤no ipv6 redirects

interface vlan 11
   ipv6 address 2001:db8:abcd:11::1/64
 ①ipv6 address fe80::1 link-local
   ipv6 nd management-config-flag
   ipv6 nd no-advertise-link-address
   ipv6 nd prefix 2001:db8:abcd:11::/64 off-link no-autoconfig
   no ipv6 redirects
```

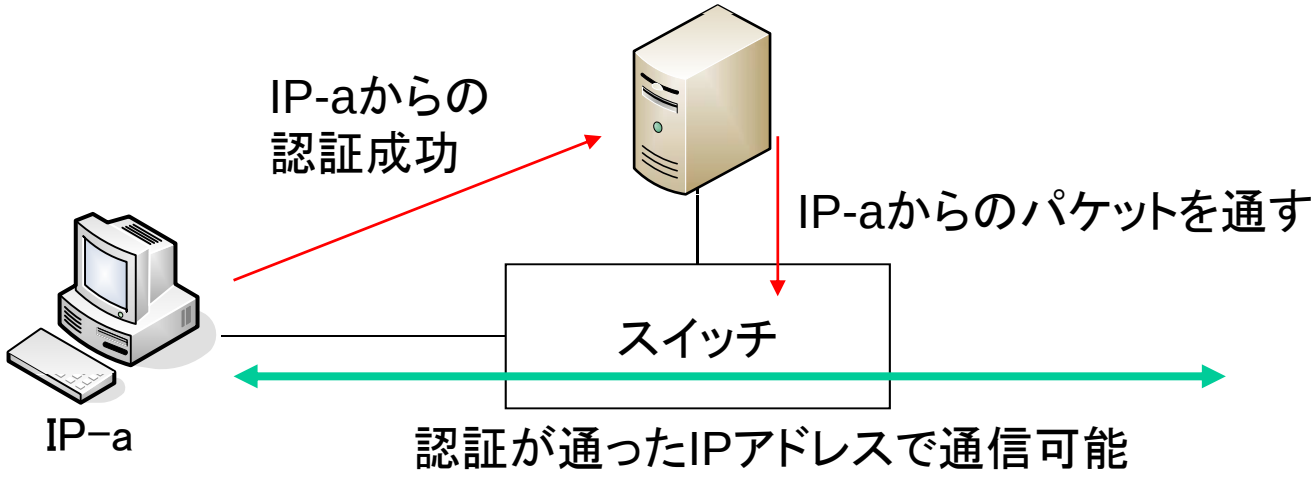
3. 端末が複数のIPアドレスを有する影響

(1)背景

既存のセキュリティソリューションの多くは「1端末1IP」を想定

e.g.)

- (MAC, IP)のペアでフィルタリングを行い、MACをキーに(MAC, IP)のペアを常時更新することで、セキュリティ確保
  →MACに対応するIPは1つしかないのが前提
- サーバ認証をパスしたソースIPでフィルタを書くことで、LANのアクセス認証を実現
  →端末はIPを1つしか持たないのが前提



3. 端末が複数のIPアドレスを有する影響

(2) 想定される脅威

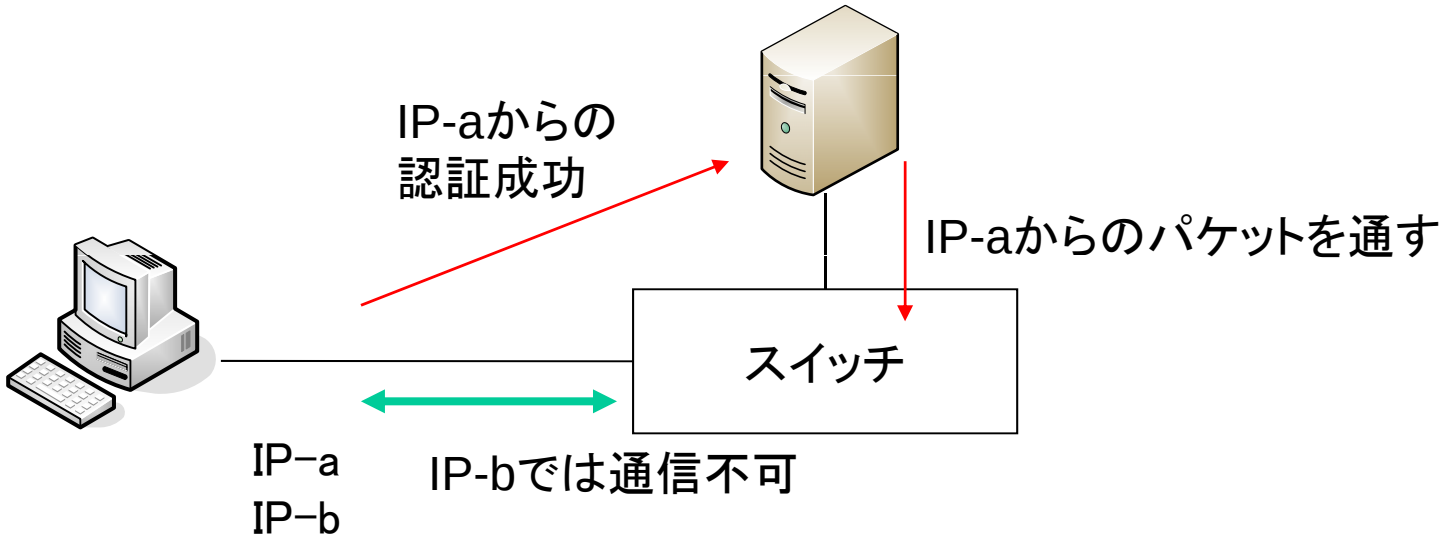
IPv6では「1端末複数IP」が当たり前になる

・IPv4アドレスとIPv6アドレス

・複数のIPv6アドレス（リンクローカル + グローバル、リンクローカル + 複数グローバル）

→既存セキュリティソリューションが成立しない恐れがある

- IPv6を導入したら、通信できなくなった
- IPv6を導入したら、意図せぬ穴が開くようになった



3. 端末が複数のIPアドレスを有する影響

(3) 対策

・本質的にはIPv4でも同じ(IPv6導入により顕在化しただけ)

・一般解はない

- 各セキュリティソリューション依存
- Layer2ベースのセキュリティソリューションは、ほとんど影響を受けないと思われる

端末が複数IPアドレスを有していたとしても、

「1端末1MAC」の前提はおそらく成り立つため

参考）IPv4/v6のプロトコル対応付け

端末収容LAN内では、IPv4・IPv6でほぼ同様なプロトコルが動作
→IPv4で行われた攻撃は、IPv6でも(理論上)実施可能

IPv4	IPv6	IPv6で想定されうる攻撃	（呼応するIPv4攻撃）
ARP	ICMPv6 (NS/NA)	ICMPv6 DoS(NS/NA)	(ARP DoS)
		ICMPv6 Spoofing	(ARP Spoofing)
DHCP	DHCPv6 (Optional)	DHCPv6 DoS	(DHCP DoS)
		DHCPv6 Spoofing	(DHCP Spoofing)
	ICMPv6 (RS/RA)	ICMPv6 DoS(RS/RA)	(DHCP DoS)
		ICMPv6 Spoofing	(DHCP Spoofing)
IGMP	ICMPv6 (MLD)	ICMPv6 DoS(MLD)	(IGMP DoS)
ICMP Redirect	ICMPv6 (Redirect)	ICMPv6 DoS(Redirect)	(ICMP DoS)
		ICMPv6 Spoofing(Redirect)	(ICMP Spoofing)