FIT2010パネルセッション
IPv6移行時におけるセキュリティ対策の展望
ー予測不能なサイバー攻撃に備えるためにはー

IPv6移行時に注意が必要なセキュリティ上の脅威と対策
ー実装者の観点からー

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

はじめに

IPv6は、一部プロトコルの挙動は若干違うが、基本的にはIPv4と同じ

→ 基本的にはIPv4のセキュリティ対策が適用可能

例. TCPへの攻撃対策, Phishing詐欺対策, …

→「一部のプロトコル挙動の違い」が、既存のIPv4セキュリティ対策にどう影響するかを考える必要あり

本発表では、プロトコル挙動の違いに注目し、
IPv6が網内に入ってくると発生する
　忘れがちなポイント（＝注意すべき脅威）
を紹介します。更に、その傾向から、
　運用上注意すべきポイント(＝その対策）
を整理します。

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

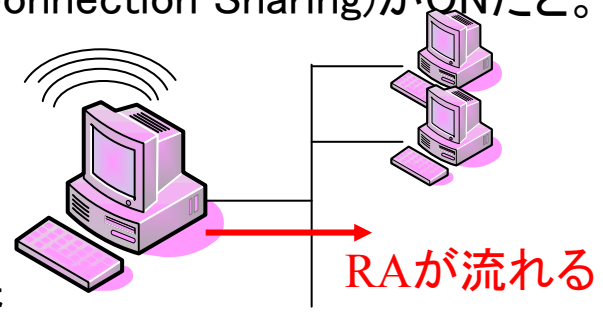
6to4 = IPv4グローバルアドレスがあれば、IPv6接続可能

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（グローバル）

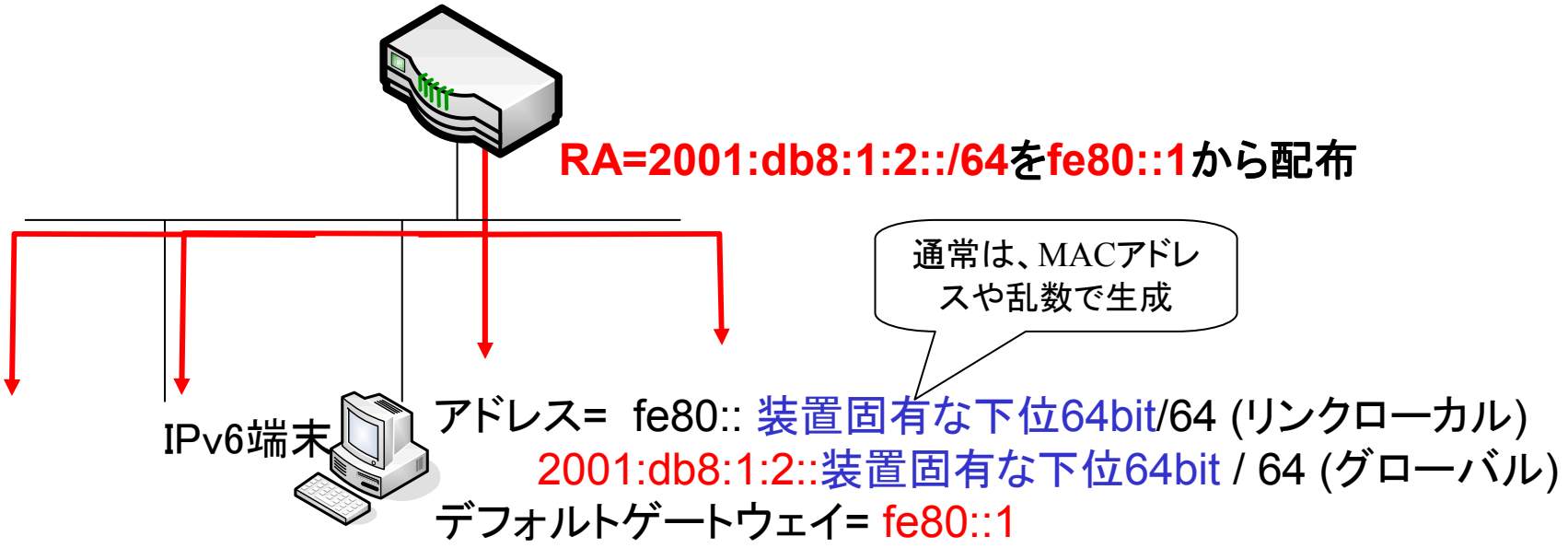
（1） 背景

・IPv6グローバルアドレス生成には、RA（Router Advertisement)が必須

※DHCPv6でもアドレス生成可能だが、DHCPv6ではデフォルトゲートウェイやPrefix長を配布できないため、事実上RAが必須

・ルータが、RAでPrefix・デフォルトゲートウェイをマルチキャストで広告
端末が、受信したPrefixからグローバルアドレス生成 + デフォルトゲートウェイ設定

1パケットでアドレス生成できるのは、DHCPに比べると単純だが。。。。

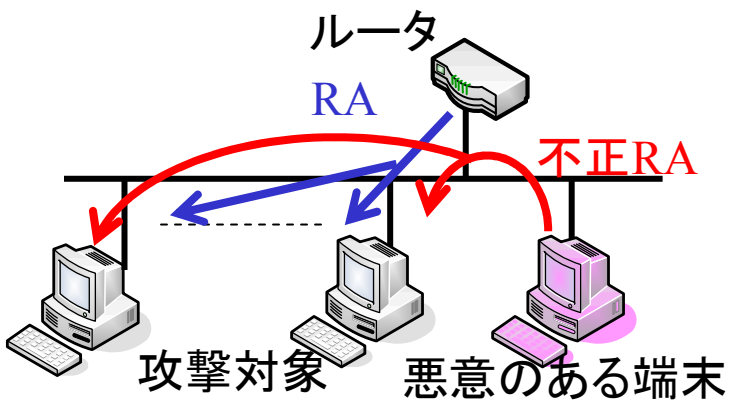


1. 意図せぬアドレス生成（グローバル）

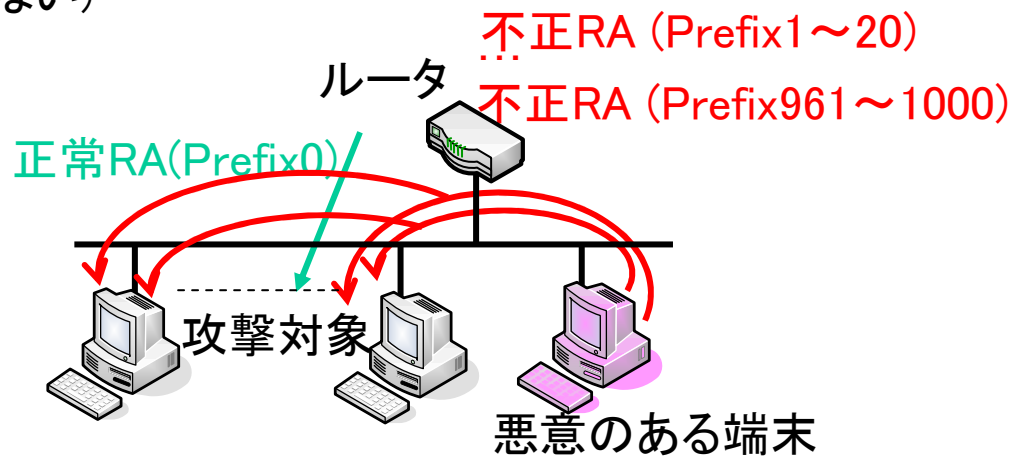
(2) RAを悪用した攻撃・脅威

・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

2. マルチキャストが漏れるLANとの相性

(1) 背景

IPv4のARPやDHCPは、事実上unicastで動く

ARP : ARP Requestはbroadcastだが、responseはunicast

DHCP: broadcastで送られるが、パケット内のxidフィールド値で自宛判定

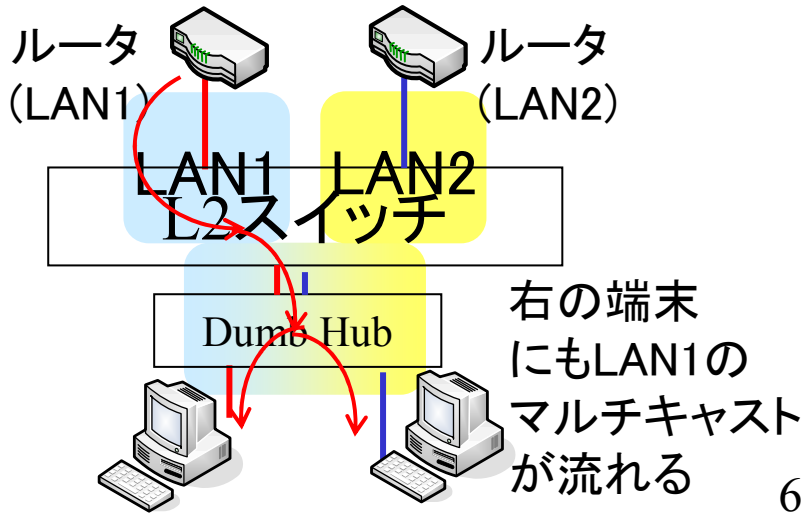
IPv6のRAは、multicastだけで動いてしまう

→今までIPv4 unicastは普通に動いていた(が実はmulticastはサブネット間で漏れてしまう) LANで、IPv6が妙な動きをすることがある

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

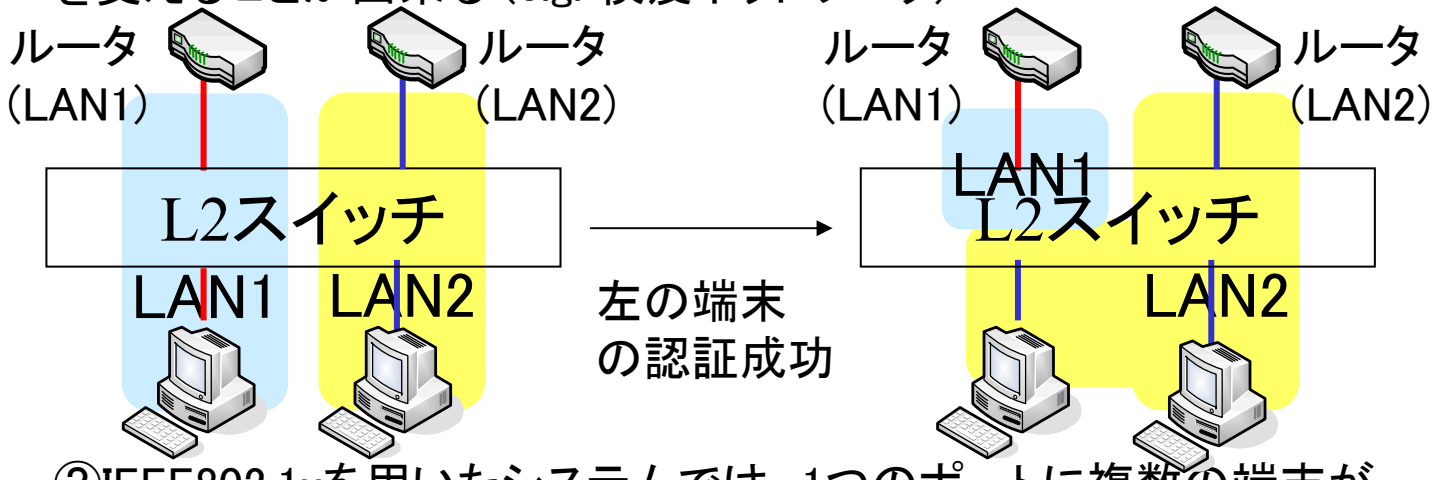
→意図せぬ通信断や不正アクセス



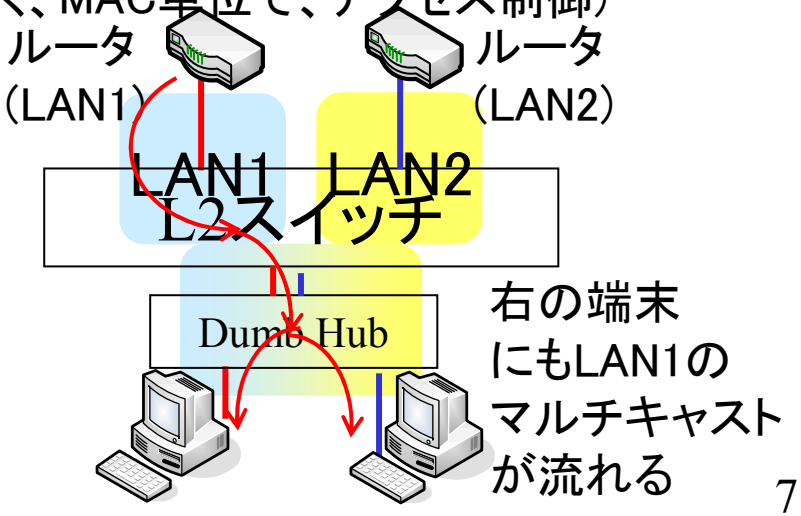
2. マルチキャストが漏れるLANとの相性

(2) 例. IEEE802.1xの認証VLAN

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



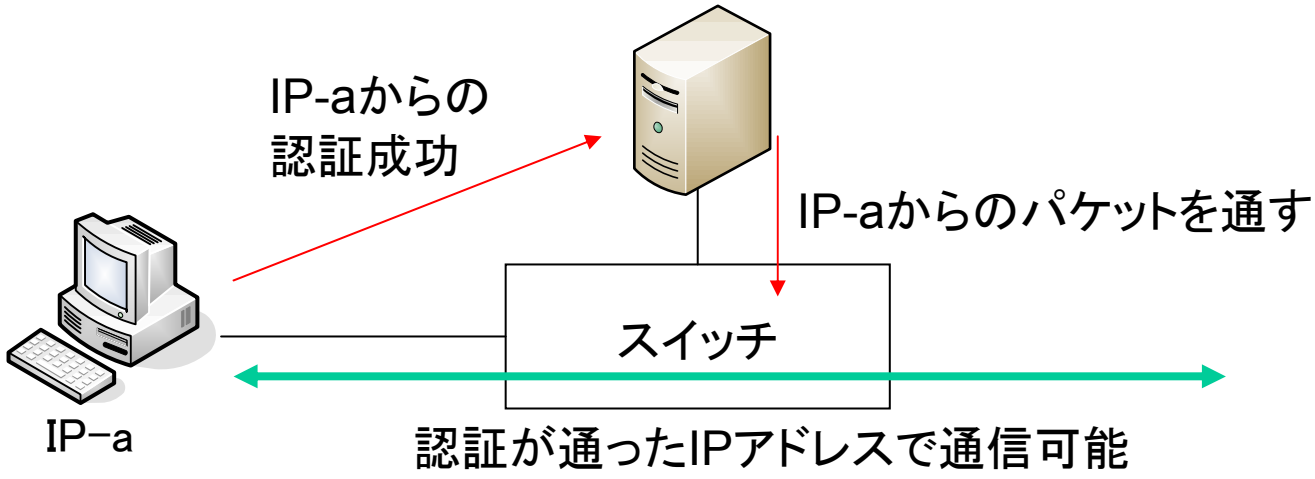
3. 端末が複数のIPアドレスを有する影響

(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

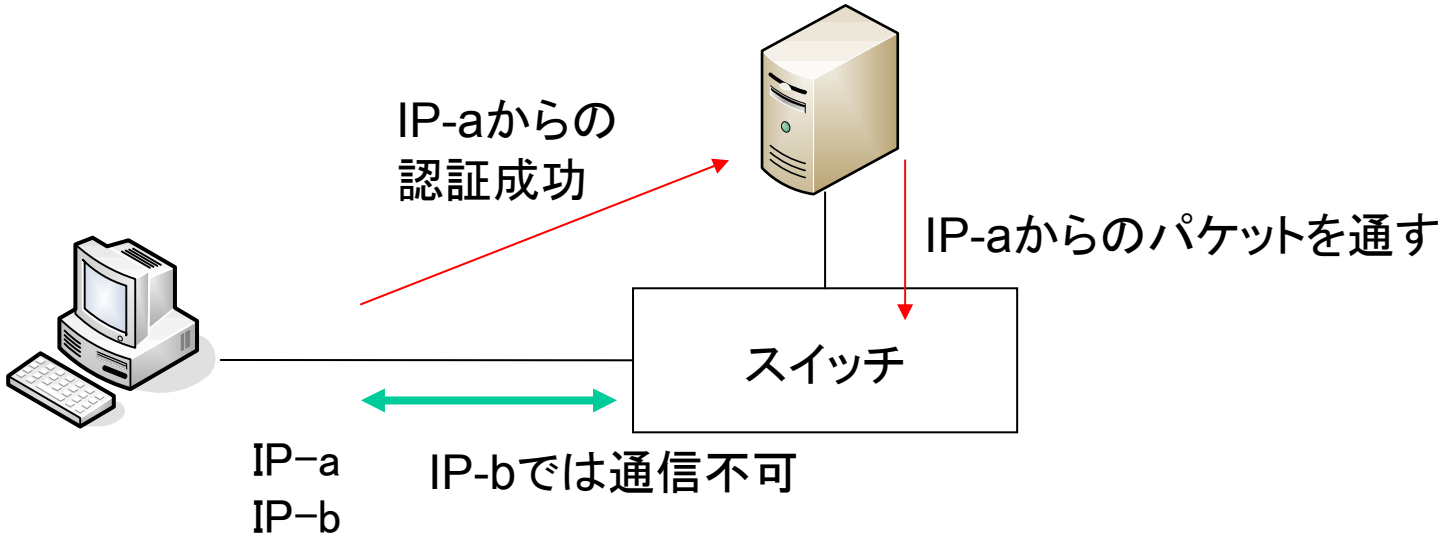
IPv6では「1端末複数IP」が当たり前になる

・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



4. 意図せぬ端末IPアドレス変更

(1)背景

・既存のセキュリティソリューションの多くは、「端末に割り振ったIPアドレスは管理サーバ(e.g. DHCPサーバ)で把握可能」と仮定

・IPv6ではPrivacy Address Extension(RFC4941)により、端末が自律的にIPアドレスの下位64bitを変更できる（匿名アドレス）

(2)想定される脅威

・前ページと同様な脅威が想定される

※変更前のIPv6アドレスで持続中の通信については、変更前のIPv6アドレスを利用し続ける（該当の通信がなくなった後で、変更前のIPv6アドレスを削除）

→ あるTCPセッションのIPアドレスが突然変わるわけではない

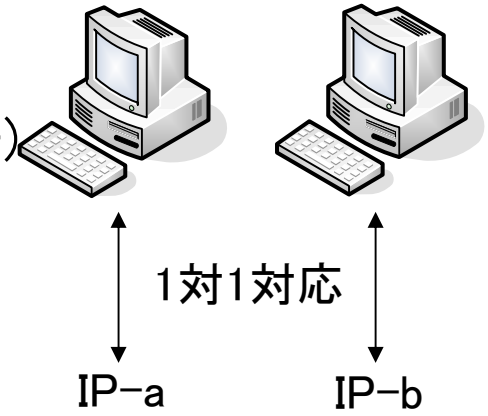
5.「端末のIPアドレス」の持つ意味が変わった

・IPv4のみの世界でのIPアドレス

2つの意味を持っていた

- Locator（経路制御上、端末がどこにあるか示す番号）
- Identifier（端末を一意に順引き/逆引きできる番号）

→「IPアドレスで端末認証」という仮定が成立した

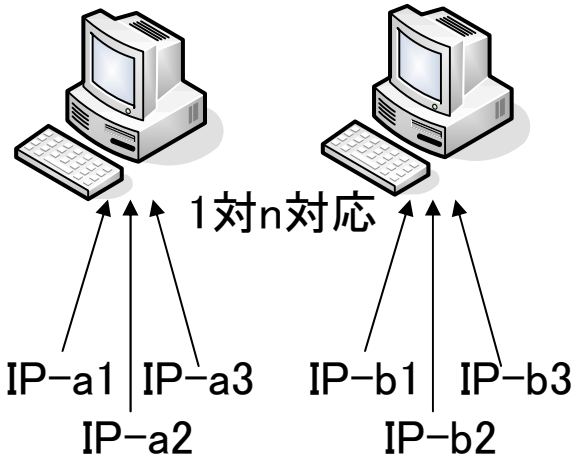


・IPv6もある世界でのIPアドレス

IPアドレスはもはやLocatorの機能しかない

（Identifierたりえない）

→「IPアドレスで端末認証」という仮定が成立しづらい



5. まとめ

・3種類のIPv6導入時の脅威

1)意図せぬアドレス生成(グローバル)

2)マルチキャストが漏れるLANとの相性

3)端末のIPアドレスは、端末のIdentifierにはならない

・いずれも、「IPv4にも潜在するが、今までの使い方では顕在化しなかった脅威」

→ IPv6が勝手に有効になる(野良IPv6)リスクを防止することが大事

→ その対策で、IPv4も安全になる

1) 本質的原因は「管理者の手の届かぬところで直接通信できること」

→端末間で直接通信をさせない (Private-VLAN, Privacy Separation)

2) そもそも「マルチキャストが漏れる」こと自体がリスク

→漏れないようにするべき

(or ユニキャスト通信だけでIPv6提供 (e.g. IPv6 over IPv4トンネル)

3) セキュリティポリシー上の「IPアドレスの意味」が曖昧なことがリスク

→ IPアドレスはLocatorとしてのみ使用すべき