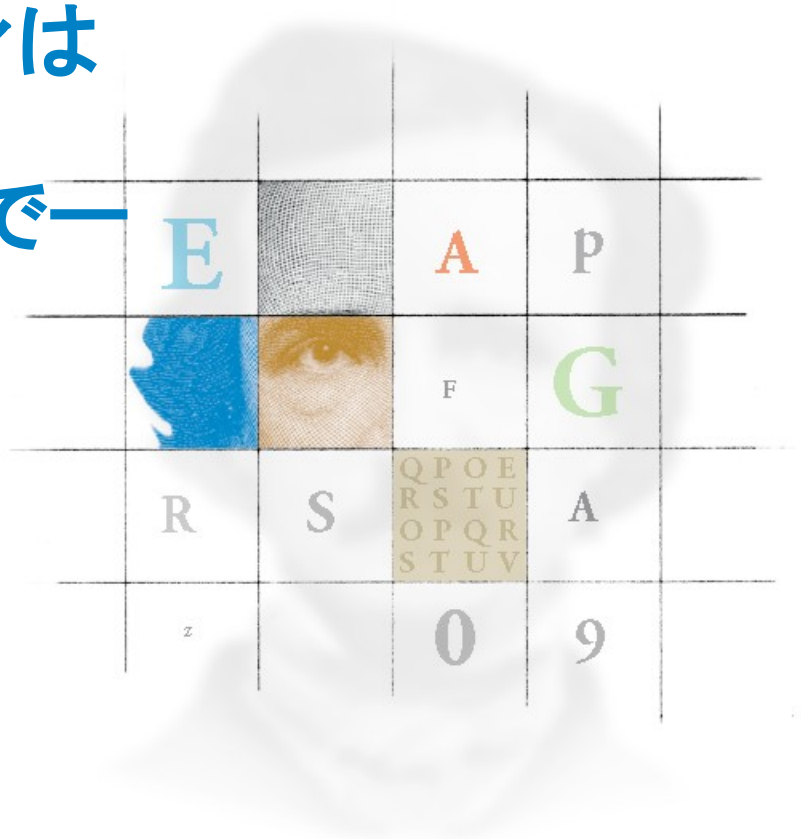
RSA CONFERENCE 2009

IPv6によってセキュリティはどう変化するか？ ―LAN上の挙動の観点で―



鈴木伸介
アラクサラネットワークス(株)

Jun 10 2009 | Session ID: RC-08

Agenda

はじめに

IPv4・IPv6で共通なセキュリティ的課題

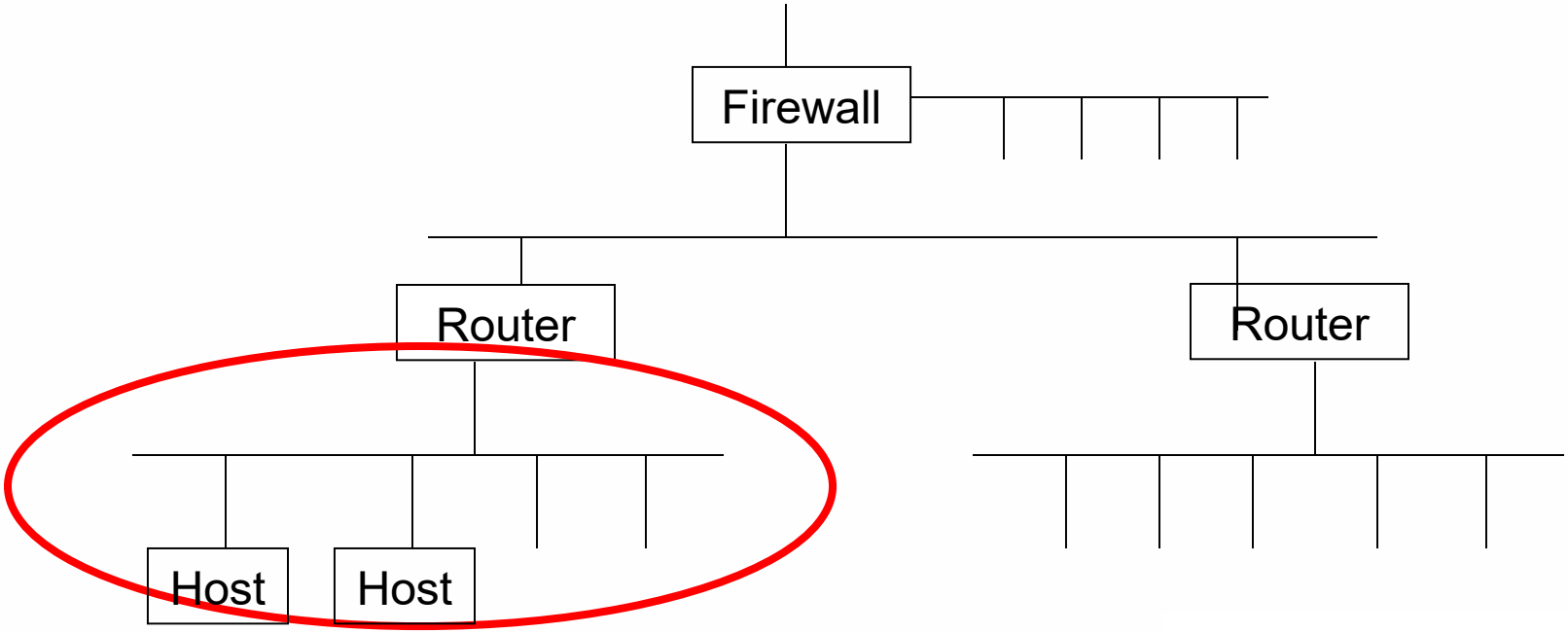
IPv6固有なセキュリティ的課題

おわりに

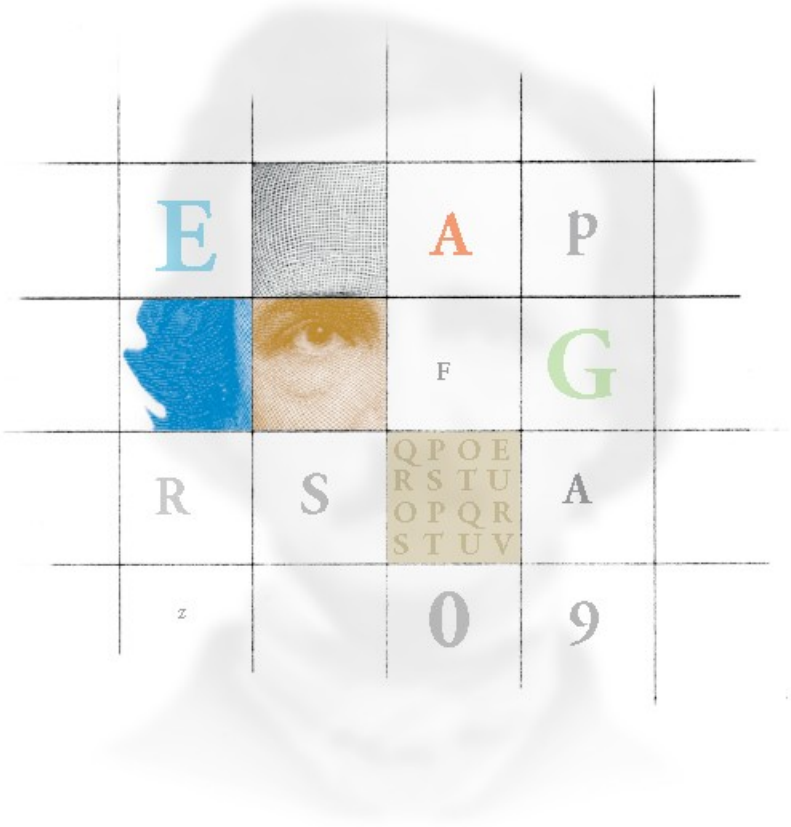
はじめに

本発表の分析対象

- 端末収容LAN/セグメント内のセキュリティ分析
  - その他観点のセキュリティ分析は別発表にてカバー
    - LAN/サブネットに閉じないセキュリティ分析
    - サーバやルータ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



IPv4・IPv6で共通なセキュリティ的課題



IPv4/IPv6とで共通な攻撃パターン

- 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)

IPv4/IPv6とで共通な攻撃への対策

- 基本的には、IPv4と同様な対策で回避可能。
  - ただしIPv6独自な対策がある場合もあり。
  - 特にLayer2ベースの対策は、IPv4/IPv6共通に適用可能

IPv6	回避策	監視強化策
ICMPv6 Spoofing	ICMPv6フィルタリング Layer2分割	ICMPv6監視　SEND Layer2認証
DHCPv6 Spoofing	DHCPv6フィルタリング DHCPv6認証 Layer2分割	DHCPv6監視 Layer2認証
ICMPv6 DoS	Rate Limiting Layer2分割	ICMPv6監視　SEND Layer2認証
DHCPv6 DoS	Rate Limiting Layer2分割	DHCPv6監視 Layer2認証

下記については、IPv6固有なため、別途考察要

- NDP(NS/NA)のうち、IPv6固有な処理
- NDP(RS/RA)
- 端末が複数のIPアドレスを持つこと

} 本発表の対象

- Path MTU Discovery (IPv4ではルータの仕事、IPv6では端末の仕事)
  → LAN内セキュリティ分析の対象外

IPv6固有なセキュリティ的課題

IPv6固有なセキュリティ的課題

下記の3項目について、内容・想定される攻撃・対策を説明

1. NDP(NS/NA)のうち、IPv6固有な処理
2. NDP(RS/RA)
3. 端末が複数のIPアドレスを持つこと

1(1) NDP(NS/NA)のうち、IPv6固有な処理

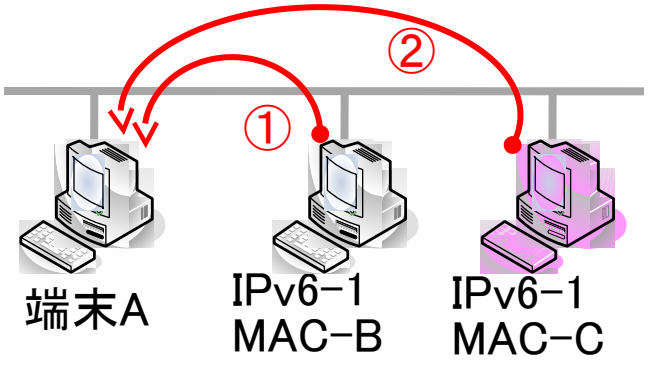
- NDP(NS/NA)が提供する機能
  - IPアドレスとLayer2アドレスの対応付け
    - 近隣キャッシュ：IPアドレスとLayer2アドレス対応を保持
      - IPv4では、ARP Request/ARP Replyに相当
    - 不到達検出機能：近隣キャッシュを最新に保つ
      - IPv4では、ARP近隣キャッシュの更新に相当
    - Anycast対応 ：LAN上の複数端末が同一IPアドレスを所有可能
      - IPv4では、対応機能無し
  - 重複アドレス検出機能
    - アドレス設定時に、アドレス重複がないか確認
      - IPv4では、Address Conflict Detection(RFC5227)に相当
        (全端末が実装しているわけではないが)

IPv6固有な処理 = Anycast対応

1(2) NDP(NS/NA)のAnycast対応の概要

- NDP応答(NA)にoverride flagを導入
  - Override bit ON = 後からNDP応答の上書OK → 通常アドレスのNA
  - Override bit OFF= 後からNDP応答の上書NG → AnycastのNA *New!!*

※IPv4のAnycast (IGP Anycast)とは全く別物 (NDP Anycast)



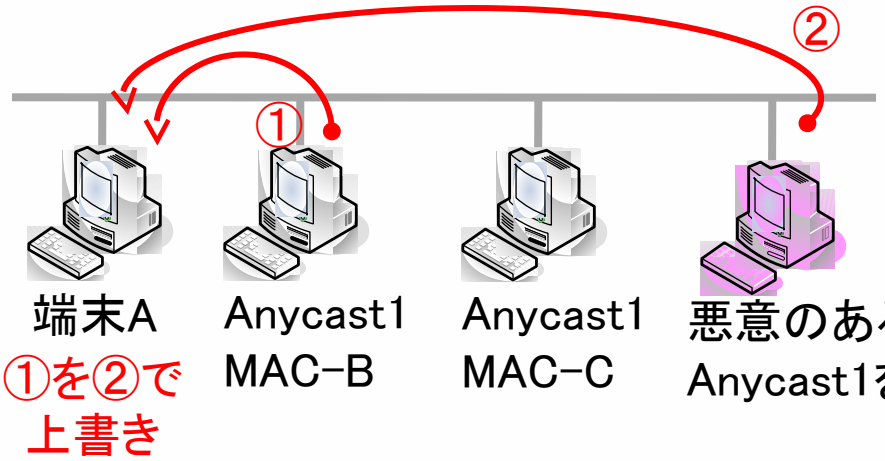
IPv6−1がAnycastの場合→

IPv6−1がAnycastの場合、端末Aは一番応答が早い端末を選択→負荷分散が可能
- Subnet Router Anycast (RFC2373)
- Mobile−IPv6 Home Agent Anycast (RFC3775)

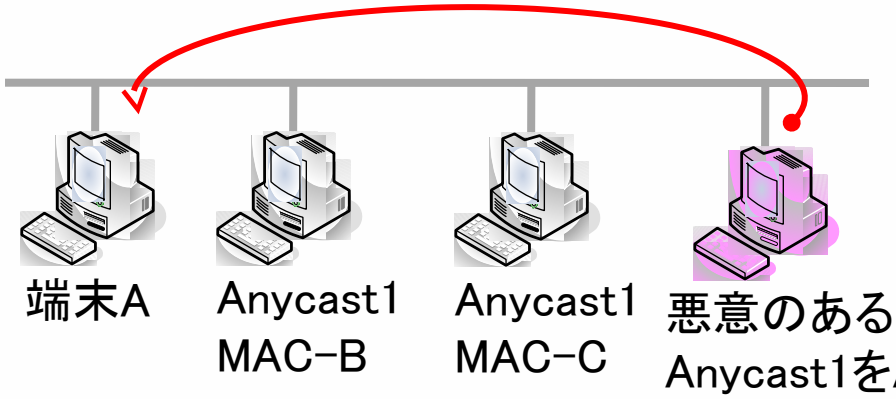
①からのNAのOverride bit	②からのNAのOverride bit	端末Aの近隣キャッシュ
OFF	OFF	MAC-B
OFF	ON	MAC-C
ON	OFF	MAC-B
ON	ON	MAC-C

1(3) NDP Anycastに対する攻撃

- NDP Anycastを前提にしたサービスを乗っ取り可能
  - Subnet Router Anycast : (特にサービスなし)
  - Mobile-IPv6 Home Agent Anycast : サービス(Mobile-IPv6)側で対策



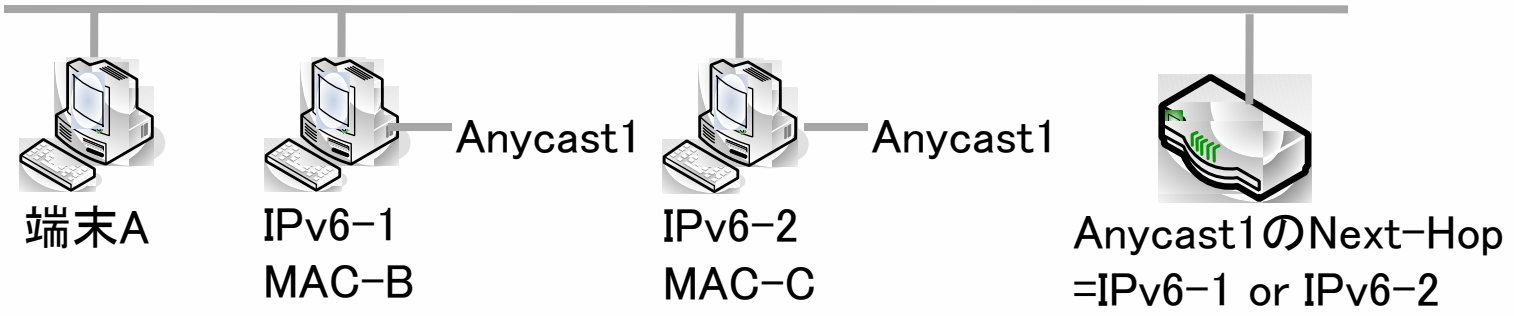
端末Aは、常にAnycast1が
MAC-Dだと思い込む



網内で、MAC-DもAnycast
提供しているように見える

1(4) NDP Anycast攻撃への対策

- IGP Anycast ならば、IPv6でも、IPv4と同様に攻撃回避可能 (RFC4786)
  - 経路制御をセキュアに提供する技術に帰着



- NDPメッセージの認証機能(SEND)でも対応可能
  - 公開鍵暗号技術を用いて、NDPメッセージ自体に署名
    - → NDPメッセージの認証が可能
    - 万が一SEND対応端末から攻撃を受けても、公開鍵情報から端末を特定可能
  - 但し以下の課題がある
    - 世の中にはSEND対応装置が少ない
    - 認証DoSが可能
- Anycastを使用しない (e.g. Subnet Router Anycastを無効に)

2(1) NDP(RS/RA)が提供する機能

- ステートレスに各種パラメータを設定
  - アドレス・デフォルト経路の設定
  - 各種リンク内パラメータの設定
    - MTU
    - TTL
    - NDP関連のタイマー値
      - 近隣キャッシュ有効期間
      - NS/NA再送間隔
      - デフォルトルータの有効期間
      - RS再送間隔
    - 各種サーバの存在の通知
      - Stateful DHCPv6 Server
      - Stateless DHCPv6 Server
      - Mobile-IPv6 Home Agent
- 上記パラメータを定期更新
  - 端末が、RS再送間隔タイマー値に基づき、定期的にRSを送信

2(2) ステートレス設定を悪用した攻撃

- 悪意のある端末から、LAN内に不正なRAをブロードキャストすることで、以下の攻撃がDHCPよりも容易に実行可能
  - 盗聴
    - 端末へ悪意のある端末経由の経路を注入

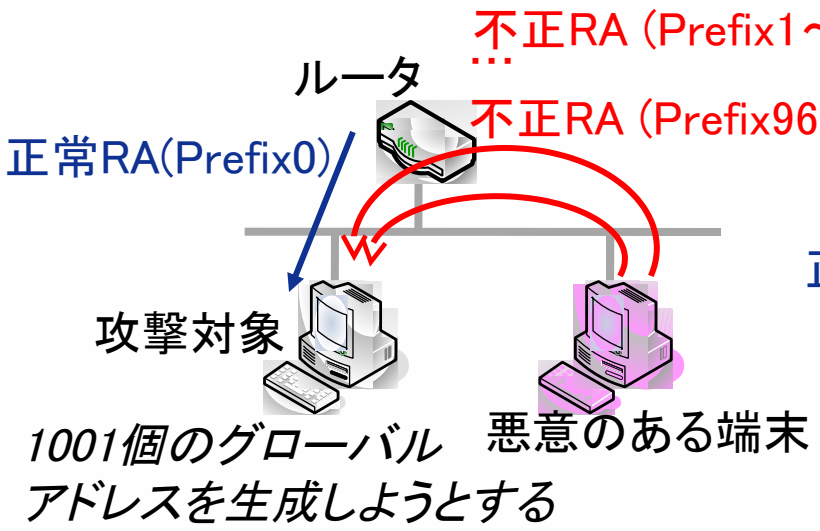
      (デフォルトルート, connected route, static route)
  - 通信停止
    - 端末へ存在しないルータ経由の経路を注入
    - 低すぎるTTL値を注入
    - Router Lifetime=0を注入
  - 偽装サーバの使用を強制
    - DHCPv6サーバへの問い合わせを誘導し、不正DHCPv6サーバから偽DNSサーバを広告

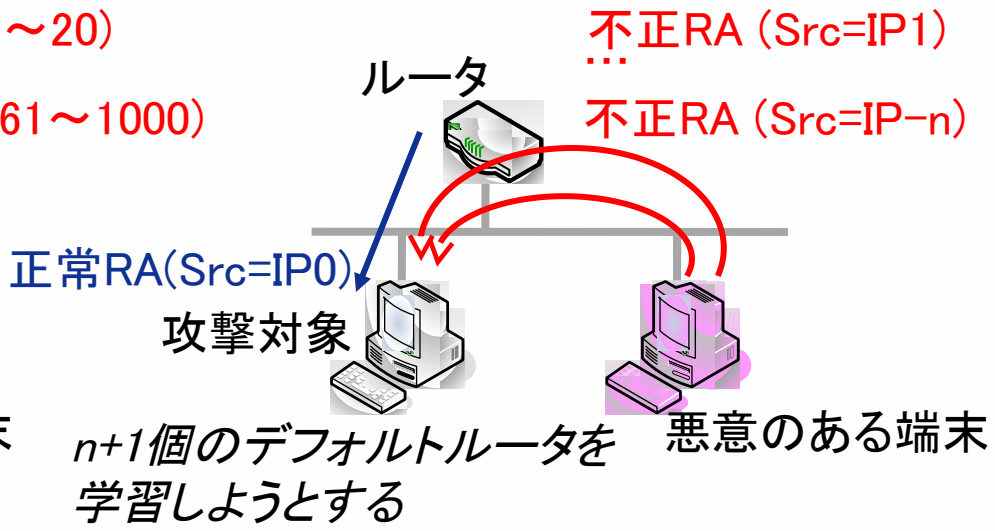
※DHCPv4でも同様な攻撃が可能だが、RS/RAでは、1RAメッセージでLAN内全てを攻撃できる分、攻撃の効果が大きい。

2(2) ステートレス設定を悪用した攻撃(cont.)

- 複数種類のRAをLAN内で広告することで、DoSが可能
  - プレフィックスを大量に学習させる
  - デフォルトゲートウェイを大量に学習させる

…





※DHCPv4では情報配布元が1サーバに限定される仕様であるため、同様な攻撃は困難

2(3) ステートレス設定を悪用した攻撃の対策

- DHCP Spoofingと同様な対策で大丈夫
  - Layer2分割
  - RAパケットのフィルタリング
  - RAパケットの監視
- NDPメッセージの認証機能(SEND)でも対応可能

  1(4)と同様
- 端末側でRAによる学習パラメータ数の上限を設けられる方がよい

3(1) 端末が複数のIPアドレスを有する影響

- 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

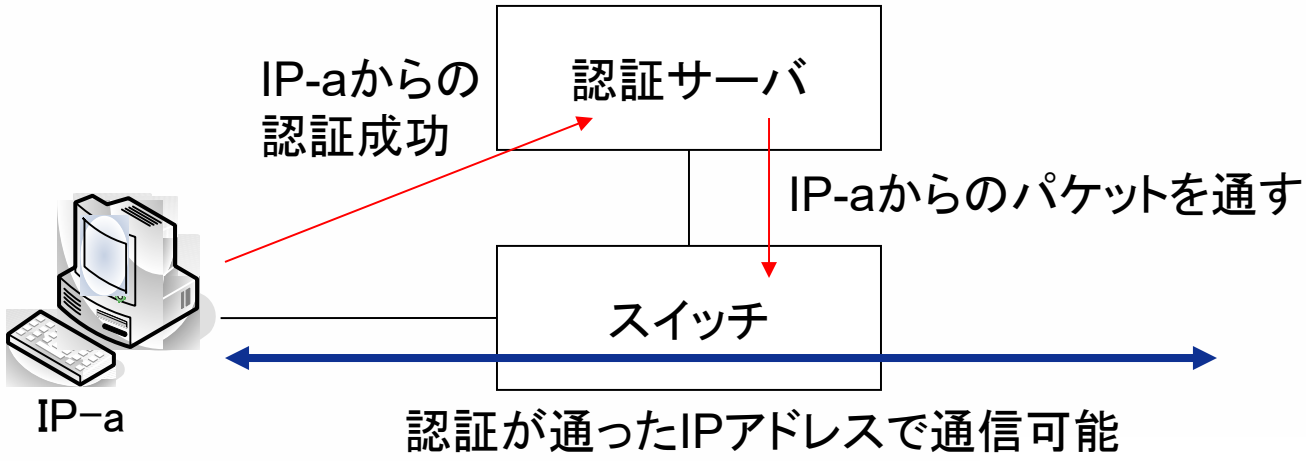
  e.g.)

  - (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



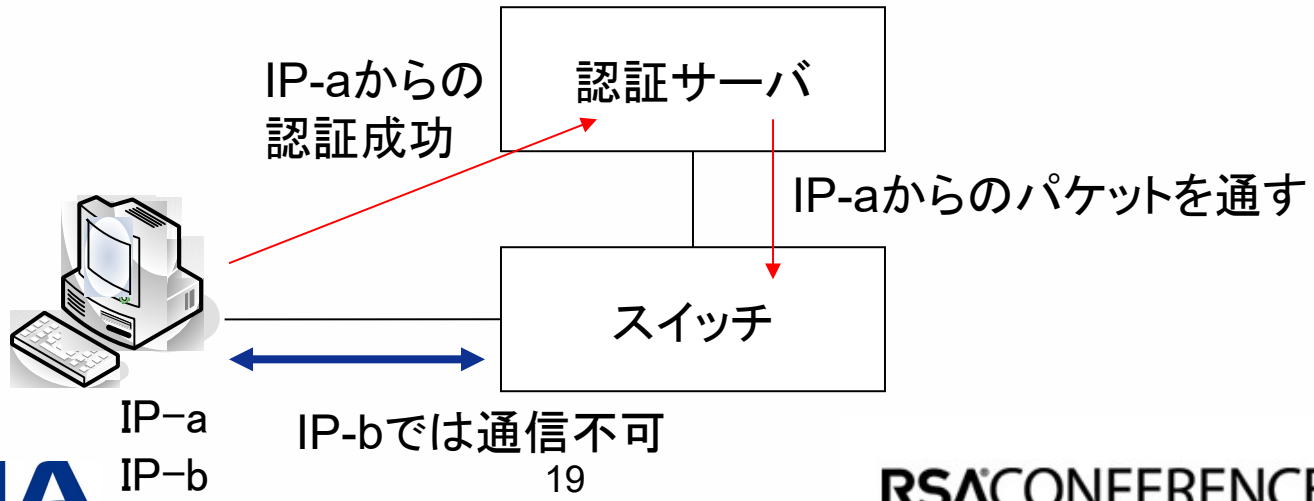
3(1) 端末が複数のIPアドレスを有する影響 (cont.)

- 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崩壊する恐れがある

e.g.)

- 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(2) 端末が複数のIPアドレスを有する影響の回避策

- 本質的にはIPv4でも同じ問題がある
  - 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

おわりに

まとめ

- IPv6でも、IPv4 ARP/ICMPセキュリティ対策と同様な対策が有効
- 1端末が複数のIPアドレスを所有することが最大の課題となると思われる
  - Layer2ベースのセキュリティソリューションならば、あまり影響を受けない
  - Layer3ベースのセキュリティソリューションの場合は、要注意