点検! IPv6のセキュリティ
ーDNSとアプリケーションー

力武 健次

NICT インシデント対策グループ

Internet Week 2009 Session H5
24-NOV-2009

NiCT 情報通信研究機構
National Institute of Information and Communications Technology

本発表の概要

- はじめに: 本発表での分析対象
- IPv4からIPv4+IPv6への移行に伴うDNSの変化
- DNSのIPv6対応によるアプリケーションの課題
- 本発表のまとめ
- 質疑応答

はじめに: 本発表での分析対象

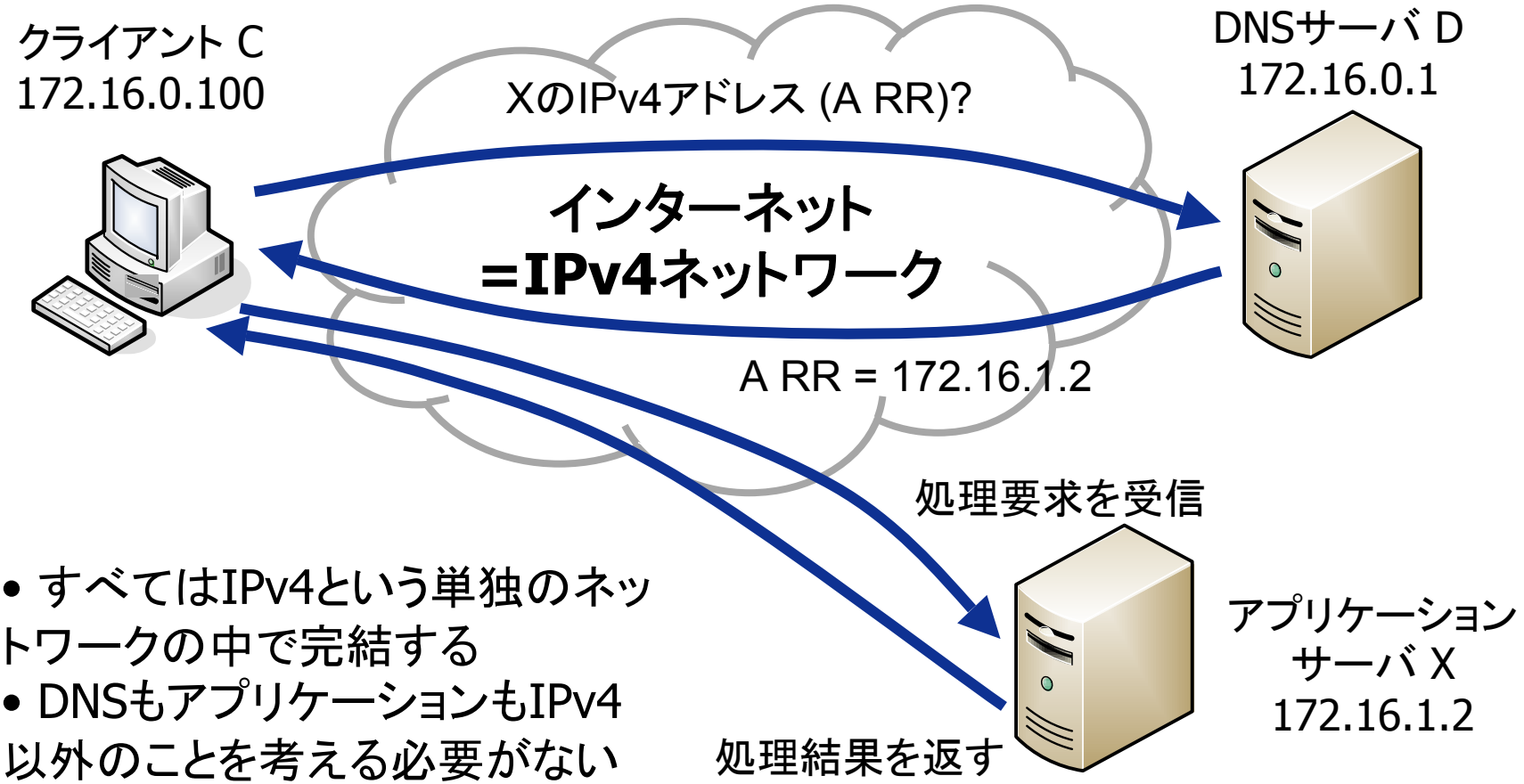
- DNSやその他のアプリケーションのIPv6対応に伴うセキュリティ問題の分析
  - 他の観点から見たセキュリティ問題は別の発表でカバー
- **IPv4とIPv6の併存環境**でDNSはどう変わるか
  - IPv4とIPv6の両方にアプリケーションは対応しなければならない
- IPv6対応でDNSやアプリケーションに出る影響

IPv4から
IPv4+IPv6への
移行に伴う
DNSの変化

Internet Week 2009 Session H5
24-NOV-2009

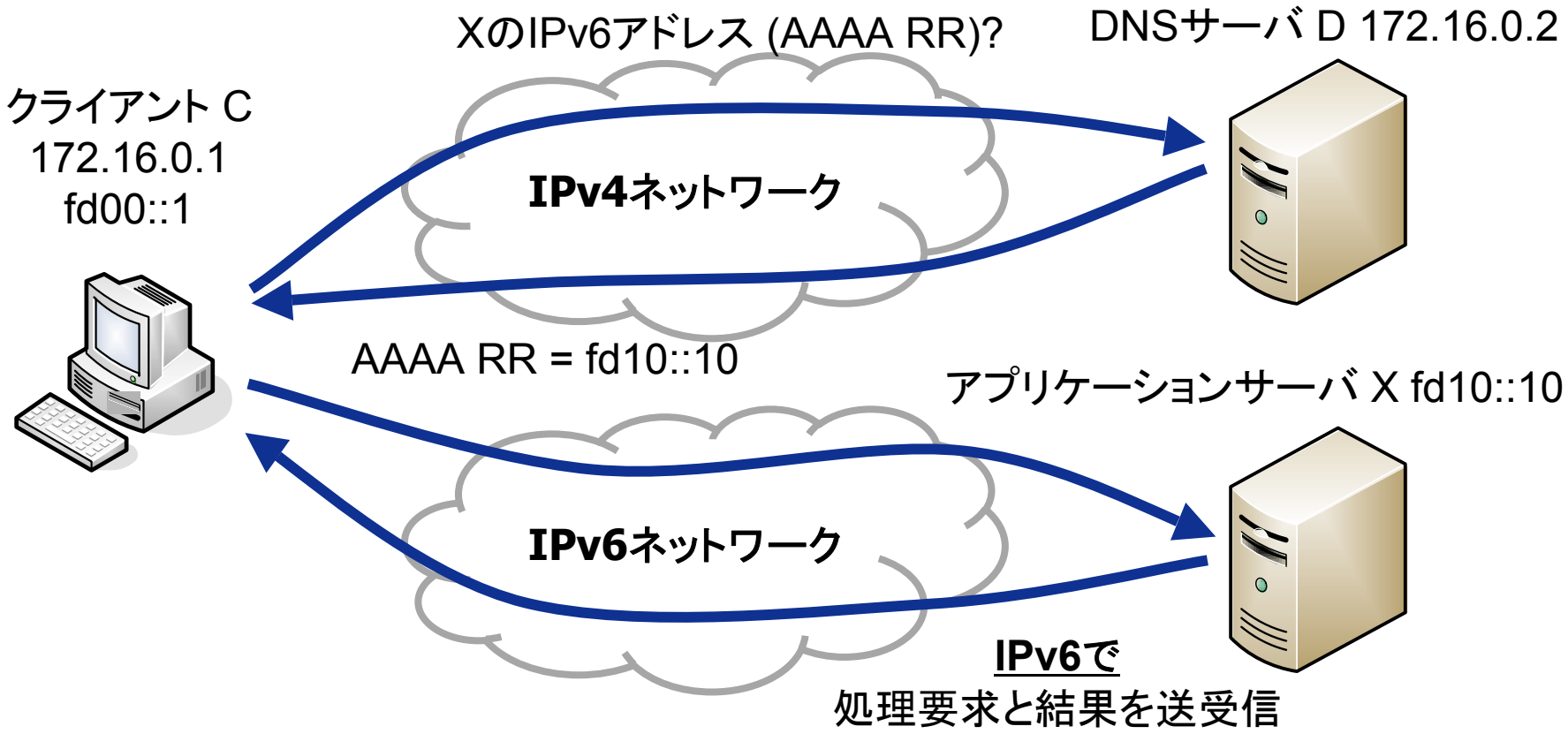
NiCT 情報通信研究機構
National Institute of Information and Communications Technology

インターネット=IPv4であった時代



- すべてはIPv4という単独のネットワークの中で完結する
- DNSもアプリケーションもIPv4以外のことを考える必要がない

インターネット=IPv4+IPv6の時の一例



- **インターネット接続ではもはや単一ではなく<u>複数ネットワークを扱う必要</u>がある**
- IPv4/v6どちらを経由して処理要求が来るかサーバ側では予測できない
- DNSではIPv6アドレスに関する情報をIPv4経由で聞いたりその逆もあり得る

DNSでのIPv6関連拡張

- アドレス記述と逆引きのみ
- AAAA RR
  - IPv4のA RRに相当，128ビットのIPv6アドレスを返す
- ip6.arpa がPTR RRによる逆引きに使われる
  - 4321:0:1:2:3:4:567:89ab → b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.ip6.arpa
- 詳細記述: RFC3596 を参照

IPv4/v6両方のアドレスを解決するには

- IPv4だけの時代はA RRだけ聞けばよかった
- IPv4/IPv6になるとA/AAAA両方聞く必要がある
  - 問題は聞いてみるまでは存在するかどうかはわからないこと
- 基本的にIPv4/v6両方あるときはIPv6優先で使う
  - アドレス解決のポリシーテーブル（RFC3484）のデフォルト設定
  - Vista, FreeBSD, Ubuntuなどはこの設定になっている
- 聞くときにIPv4/v6どちらを使うかはルールはない
  - IPv4しかDNSでは使えないクライアントもある（例: WindowsXP）
  - DNSサーバはIPv4で接続可能にしておくべき（RFC3901）

IPv6の逆引きとセキュリティ

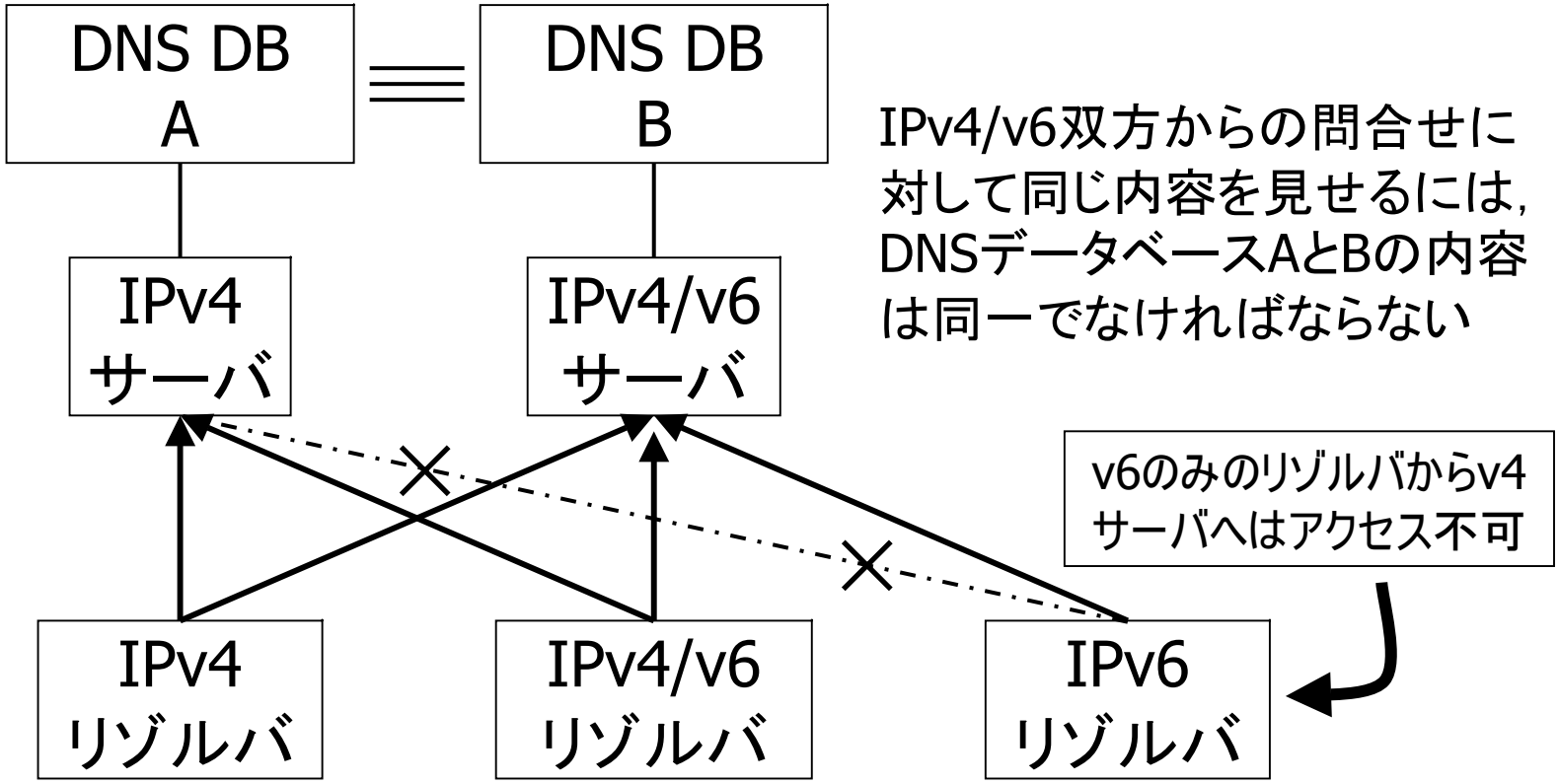
- 逆引きは認証手段としてはとても弱い
  - DNSパケットはDNSSECを使わない限り偽造可能
- そもそもすべてのアドレスが正引きに登録されるか?
  - 複数アドレス，複数プレフィクスが日常的になる
  - リンクローカルアドレスは複数サブネット間で重複するため登録不可
  - 一時アドレスは時間と共に変わっていくため更新に手間がかかる
  - →結局自動動的更新のコストとのトレードオフで考えるべき?
- 基本的に逆引きは登録されない前提で考えるべき
  - 例外: SMTPのReceived: ヘッダに書かれるホスト名など

IPv6対応OSがIPv6接続をしていない時

- IPv6対応OSがIPv6の接続性を持たない場合，DNSの名前解決が原因でアクセスが遅くなったり，不可能になったりすることがある
  - AAAA RRによるIPv6アドレスを得たがアクセスできないため，アプリケーション間接続ができずタイムアウトしてしまう
  - 上記タイムアウトでA RRによるIPv4アドレス解決にフォールバックする動作を行わない場合，IPv4の接続性があっても接続できない
- 「IPv6の機能を削除」するのは本質的解決ではない
  - AAAA RRの問合せのちょっと後（0.5秒）にA RRの問合せを並行して送るなど，DNS側でもIPv6の接続性がなかった時に備えた対策が必要（RFC4472 Section 5.1）

DNSサーバで提供するコンテンツの問題

- 同じドメイン名に対してIPv4/v6両方のアクセス経路がある限り，どちらも同じ内容を返す必要がある



IPv6関連RRによるDNSへの課題

- RRサイズの増大に伴うUDPパケット長の増大
  - AAAA RRはA RRより12バイト大きい
  - DNSSEC化に伴いこの問題はより深刻になる
  - 従来の512バイト制限ではすべてのルートサーバを収容できない
- UDPフラグメントが転送できることが前提になる
  - エンドノードのファイアウォールで転送が禁止されていることも多い
- TCPでの問合せも送受信できるようにしておく
  - UDPだけでとりあえず動いているシステムが少なくない
  - TCPでのDNS通信を禁止しているファイアウォールの設定も多い

DNSの
IPv6対応による
アプリケーションの課題

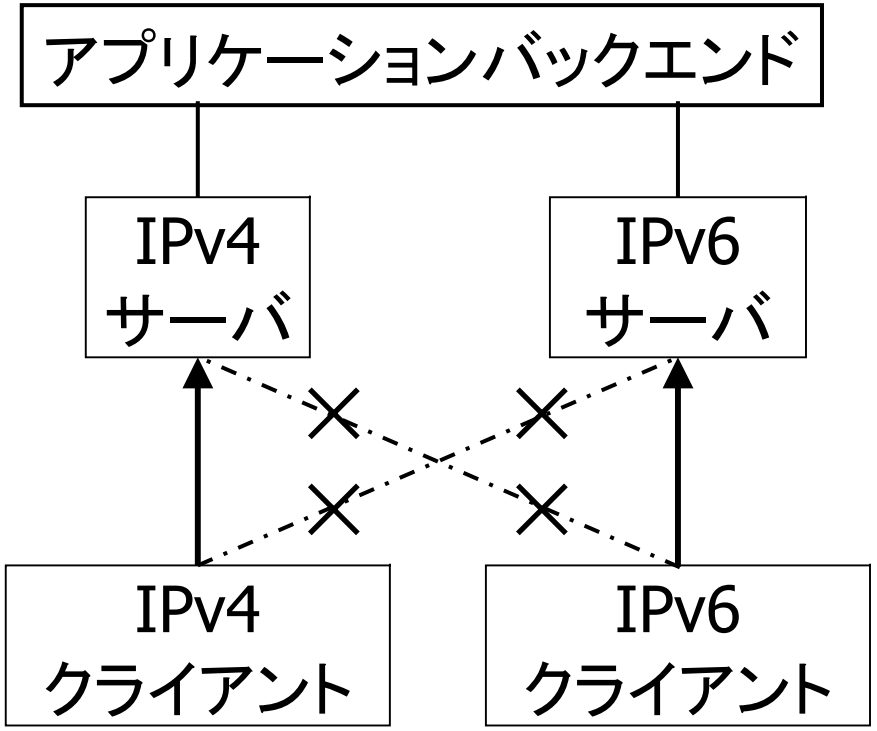
Internet Week 2009 Session H5
24-NOV-2009

NiCT 情報通信研究機構
National Institute of Information and Communications Technology

IPv4/v6併存環境でのサーバ構成

- 同じサービスに対してIPv4/v6で到達でき，かつどちらも同じサービスを行う必要がある

- プログラミングの観点からは，IPv4/v6をそれぞれ別のサーバとして構成した方が間違いが少なくなると考える
- IPv4/v6を同じソケットで受けることはBSD系OSでは推奨されない（RFC3493 Sect. 5.3）
- IPv4とIPv6という「2つのネットワーク」に対応すると考える



IPv4/v6のアプリケーションでの順位付け

- 確固たるルールは決められていない
  - 条件が悪い場合フィッシング詐欺同様の事態になることがあり得る
    - 同じ名前にIPv4/v6双方の実体が対応づけられるため，両者で提供される内容が同じでないと，XSSのような事態が発生し得る
- 3つの場合を想定する必要がある
  - 1) IPv4のみ 2) IPv4+v6（デュアルスタック） 3) IPv6のみ
  - いずれの場合でも遅延なく同じように動作する必要がある
- IPv4とIPv6両方が利用可能な場合はどちらを選ぶ?
  - RFC3484のデフォルト設定に従えばIPv6優先ということになる，が…
    - 他の選択原則を採用する場合もあり得る

IPv4/v6のアプリケーションでの順位例

- Firefoxブラウザ
  - 設定項目 network.dns.ipv4OnlyDomains
    - IPv6機能を有効にしていても特定のドメインだけIPv4のみで接続する
    - かつてdoubleclick.netではAAAA RRの問合せが無視されていたらしい
- DNSキャッシュサーバunbound
  - do-ip4 / do-ip6 オプションで機能の有無を決められる
  - 問合せの受信 / 送信に分けて選べる設定はない
- メールサーバ
  - PostfixでもsendmailでもIPv4/IPv6を使うかどうかは選べる
  - PostfixではoutgoingconnectionはIPv6優先に固定

本発表のまとめ

NiCT 情報通信研究機構
National Institute of Information and Communications Technology

本発表のまとめ

- IPv6の追加により，複数のネットワークに対して DNSやアプリケーションは対応する必要がある
- DNSや各アプリケーションで，IPv4/v6が両方使える場合の優先順位は決められていない
  - RFC3484は参考にはなるがアプリケーション層の順位は規定しない
- IPv4/v6双方で提供するデータやサービスの内容は DNSやアプリケーションで一致させる必要がある
  - 整合性が取れないとXSS同様のセキュリティ問題になる
- 参照RFC: 4472, 3901, 4942, 3484, 5220

ご清聴
ありがとうございました

NiCT 情報通信研究機構
National Institute of Information and Communications Technology