DNSOPS.jp
DNS Operators Group, Japan

DNSOPS BoF：ライトニングトーク
DNS Hot Topicになりそうなこと

DNSOPS.JP
石田慶樹

これからDNSでホットになりそうな話題

- DNSの話題はDNSSECのみにあらず
- 今後ホットになりそうな話題
  1. デュアル環境下での家庭用ルータのDNSの挙動
  2. DNSとブロッキング

→どちらも議論が始まっています

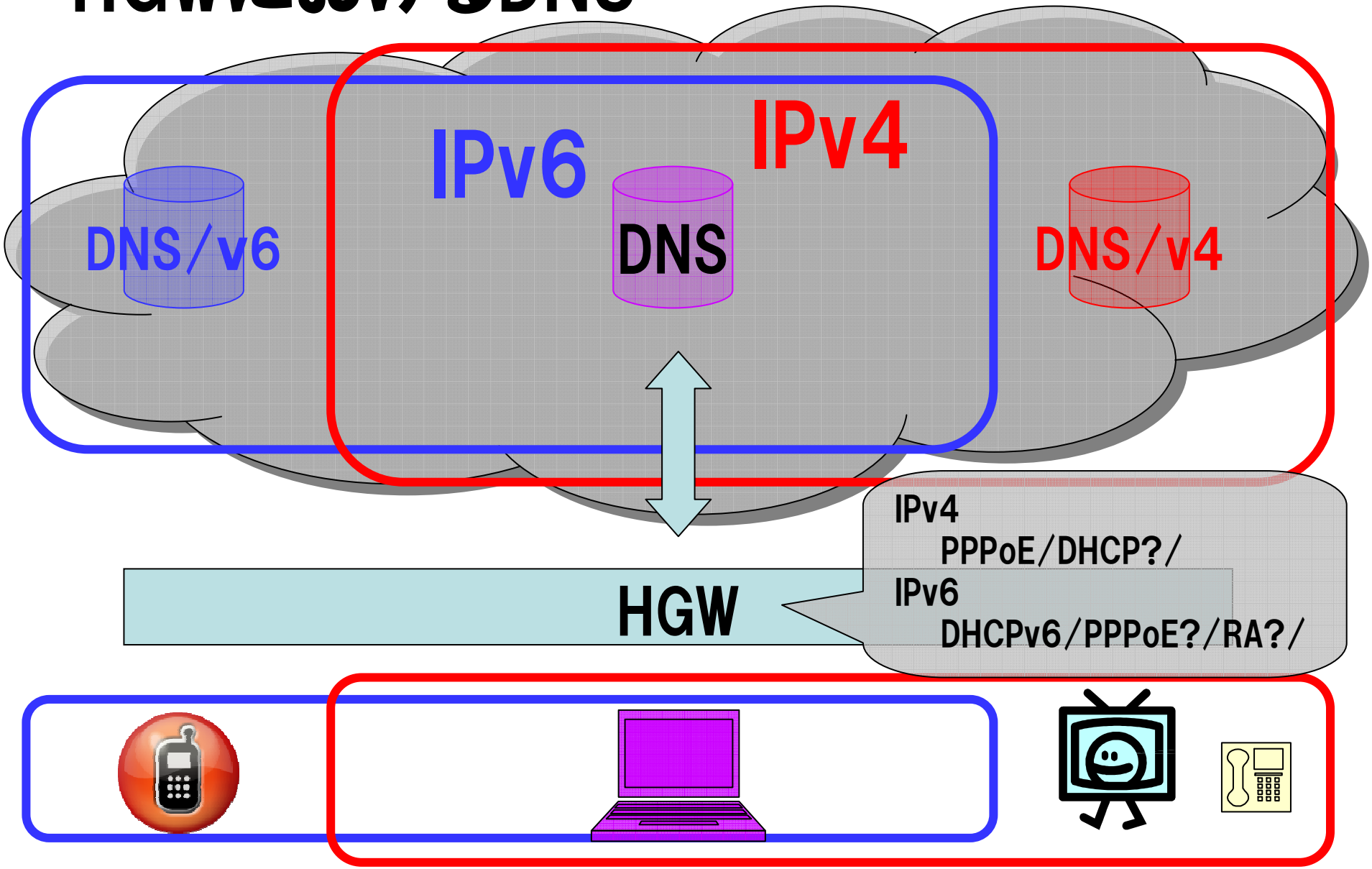
家庭用ルータにおけるDNSの挙動

- 家庭用ルータ (ブロードバンドルータ, HGW)
- これまで
  - (主に) IPv4にのみ対応
  - 簡単なキャッシュDNSの機能
  - 特に問題はなかった
- これから
  - プロバイダ側のIPv6への対応
  - DNSSECへの対応
  - 宅内環境のデュアル化への対応

家庭用ルータにおけるDNSの挙動

- DNSの観点から家庭用ルータは今のままで大丈夫か？
  - IPv6/IPv4のデュアル環境
  - EDNS0
  - TCP fallback
  - DNSSECのValidator
  - ブラウザの先読み問題
- ちょっと考えておかないとやばいかも
  - 家庭用ルータ関係者へのインプット

HGWにおけるDNS


IPv6
IPv4
DNS/v6
DNS
DNS/v4
HGW
IPv4
PPPoE/DHCP?/
IPv6
DHCPv6/PPPoE?/RA?/

HGWのDNSで考慮すべき課題

DNSOPS.jp
DNS Operators Group, Japan

ケース1:

- HGWはDNSの機能を持たない
- 端末にはHGW自身がISPから教えられたキャッシュサーバのアドレスを通知する
  - ケース1.1:
  - –HGW自身にv4 [v6] のDNSキャッシュサーバエントリがある場合
  - –トピック
    - HGWにv4 [v6] のDNSキャッシュサーバを通知しないといけない
  - ケース1.2:
  - –HGW自身にv4 [v6] のDNSキャッシュサーバエントリがない場合
  - –トピック
    - 宅内にv4 [v6] でしかDNSクエリが出せない端末はDNSを牽けない

DNSで考慮すべき課題

DNSOPS.jp
DNS Operators Group, Japan

ケース2：
- DNSのプロキシ機能のみを持つ
- 端末にはHGW自身の宅内アドレスを通知
- DNSクエリはそのまま上位キャッシュサーバに転送する

  ケース2.1：

  –HGW自身にv4 [v6] コネクティビティとDNSキャッシュサーバエントリがある場合

  –トピック

    - HGWにv4 [v6] のアドレスとDNSキャッシュサーバを通知する

  ケース2.2:

  –HGW自身もv4 [v6] アドレスもしくはv4 [v6] のDNSキャッシュサーバエントリがない場合

  –トピック

    - HGWにおいてv4 [v6] のDNSクエリをv6 [v4] に変換しなければならない

DNSで考慮すべき課題

DNSOPS.jp
DNS Operators Group, Japan

ケース3:

- DNSのフルリゾルバの機能を持つ
- 端末にはHGW自身の宅内側アドレスを通知

  ケース3.1:

  – HGW自身がv4/v6デュアルである場合

  – トピック

    ・ ?

  ケース3.2:

  – HGW自身にv4 [v6] アドレスがない場合

  – トピック

    ・ V4 [v6] でしか到達できない権威DNSサーバに到達できない

DNSで考慮すべき課題

DNSOPS.jp
DNS Operators Group, Japan

IPv4/IPv6環境下での挙動
＋
DNSSECへの対応/Validatorとなるかどうか
＋
アプリケーション（ブラウザ）の挙動への対応
↓
選択肢は沢山
どういう挙動が望ましいかのインプットの段階？

DNSOPS.jp
DNS Operators Group, Japan

DNSとブロッキング

DNSとブロッキング

DNSOPS.jp
DNS Operators Group, Japan

- JANOG26
- http://www.janog.gr.jp/meeting/janog26/program/blocking.html
- **詳細は楠さんの資料を参照のこと**
- **同様の内容は「第14回サイバー犯罪に関する白浜シンポジウム」にも**
  - http://togetter.com/li/27207
  - http://goo.gl/DeUC

DNSとブロッキング

- 背景
  - 社会として保護が必要な対象に対して、
  - 本人が意図せず、もしくは悪意を持った第三者に巻き込まれた結果、
  - 閲覧に適さないコンテンツを閲覧してしまうこと、
  - が発生する可能性を排除したい。

DNSとブロッキング

- ブロッキング
  - リスト作成者が作成したリストに基づき特定の内容についてプロバイダ（通信事業者）がコンテンツへのアクセスを遮断する
  - すべての加入者に適用されてしまう
- 提案されている手法
  - DNSポイズニング
  - パケットドロップ
  - ハイブリッド方式
  - 公衆送信抑止
- 課題
  - リストの管理
  - オーバーブロッキング

DNSとブロッキング

- ISPのキャッシュサーバにおいてブロッキングする対象となるFQDNに対して応答しないもしくは偽りの応答を返す
- DNSポイズニングと呼ばれている
- 欧州ではいくつかの国で実装済み
- 国内ではDNSによるブロッキングを指向しているISPも少なからずあり
  - 実効性とコストの面から
  - 他の方法を指向しているISPもある模様

DNSとブロッキング

DNSOPS.jp
DNS Operators Group, Japan

- 課題は山積
  - 実現と実装方法
  - 関係省庁による意識のずれ
  - いずれにせよ意見募集があるので運用者としてのコメントを投げることは重要
    - 会社としては無理でも個人としてはコメント可能