チュートリアル：
DNSの基本構成要素と
IPv6対応における注意点

2013年10月16日

IPv6 Summit in Kyoto 2013

株式会社日本レジストリサービス（JPRS）
堀 五月

講師自己紹介

- 氏名: 堀 五月（ほり さつき）
  - 勤務先：株式会社日本レジストリサービス
  - 所属部署：システム部
  - 業務内容：JPドメイン名の登録申請システム及び
    JP DNSの設計、構築、運用、ネットワーク管理
  - 京都との縁.. ：和歌山県出身→生来のプロトコルは関西弁
    現在のDefaultは共通語だが、本日は
    関西弁フォールバックでやらせてもらう予定

本日の内容

1. DNSの基本構成要素と注意点
   - 基本となる三つの構成要素とそれぞれの役割
   - DNSを理解・運用するにあたっての注意点
2. DNSにおけるIPv6対応～理論編～
   - DNSにおけるIPv6対応の基本
3. DNSにおけるIPv6対応～実践編～
   - DNSクライアントにおける対応
   - キャッシュDNSサーバーにおける対応
   - 権威DNSサーバーにおける対応
4. DNS/IPv6関連トピックス
   - AAAAフィルターの概要と注意点
   - GmailにおけるIPv6逆引きの必須化

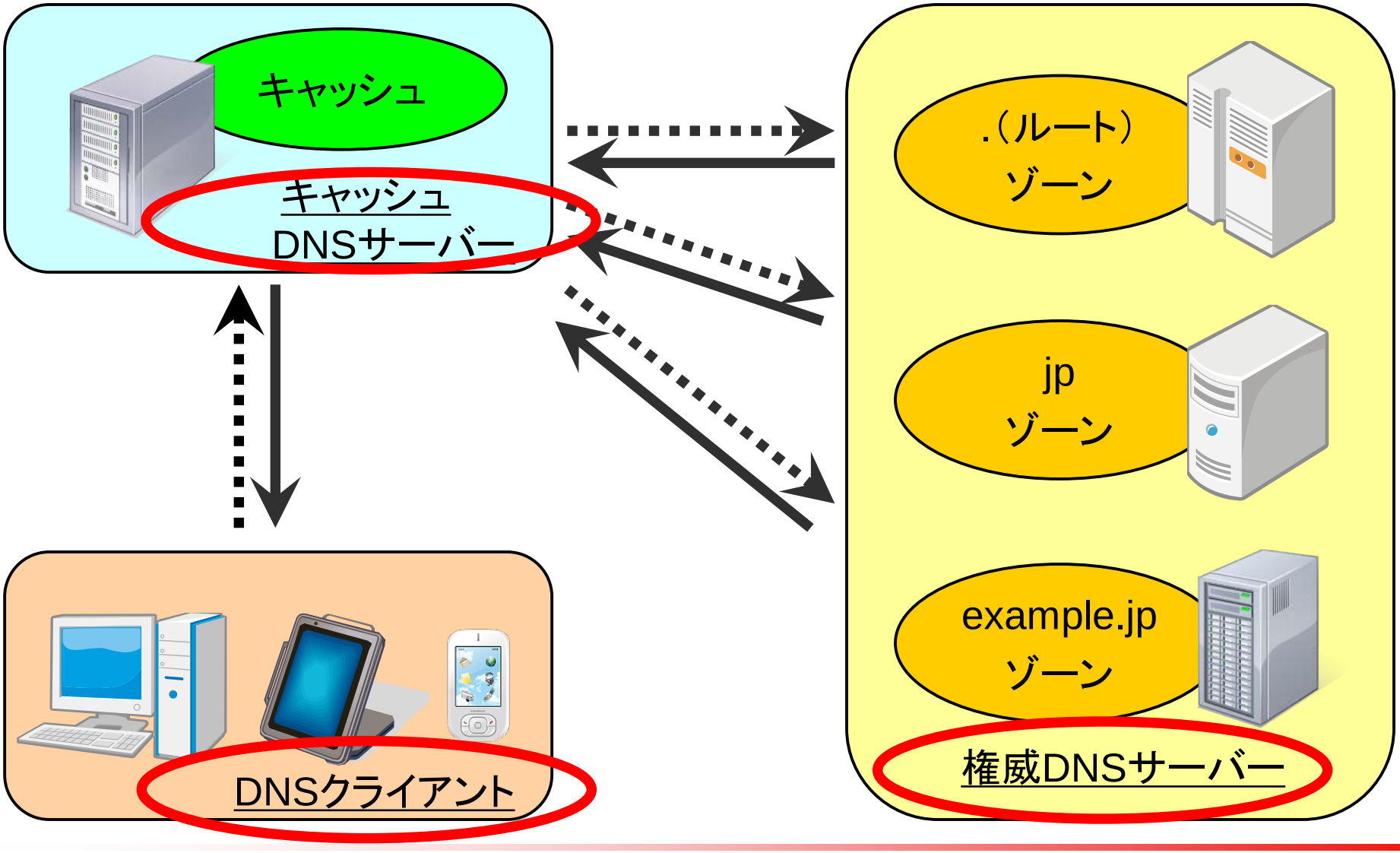
注意

- 本チュートリアルでは、ドメイン名やDNSに関する基本（入門）的な解説は行いません
  - それらについては書籍「実践DNS」や、DNS Summer Daysにおけるチュートリアル資料などをご参照ください

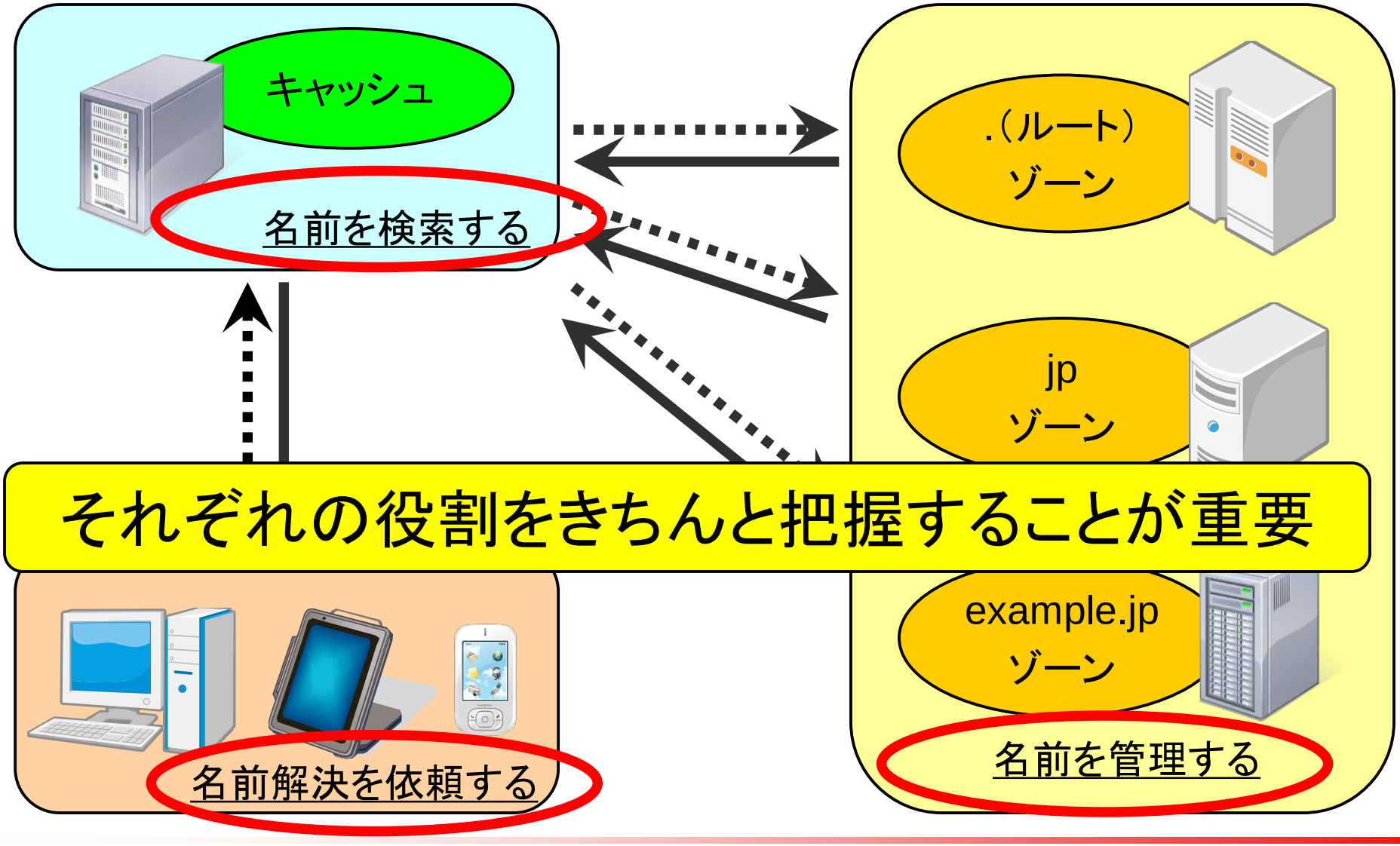
- DNS Summer Daysのチュートリアル資料は、以下のURIで公開されています
  - 2012: <http://dnsops.jp/event20120831.html>
  - 2013: <http://dnsops.jp/event20130718.html>

1. DNSの基本構成要素と注意点

DNSにおける三つの基本構成要素



それぞれの役割



それぞれの役割をきちんと把握することが重要

DNSを理解・運用するにあたっての要注意点

- 本チュートリアルでは、特に重要な以下の4点について解説
  - ① 構成要素に関する名称の不統一
  - ② 二種類のDNSサーバーの存在
  - ③ 二種類の問い合わせの存在
  - ④ 兼用可能な実装の存在

注意点①:
構成要素に関する名称の不統一

- 構成要素を表現する用語が、統一されていない
  （例）
  - DNSクライアント
    - スタブリゾルバーなど
  - キャッシュDNSサーバー
    - フルリゾルバー、フルサービスリゾルバー、参照サーバーなど
  - 権威DNSサーバー
    - DNSコンテンツサーバー、権威ネームサーバー、ゾーンサーバーなど
- 技術者、専門家の間でも表現に違いがあり、混乱しやすい
- 日本語だけでなく、英語でも統一されていない

どの「構成要素（機能）」を指しているかについて意識する必要がある

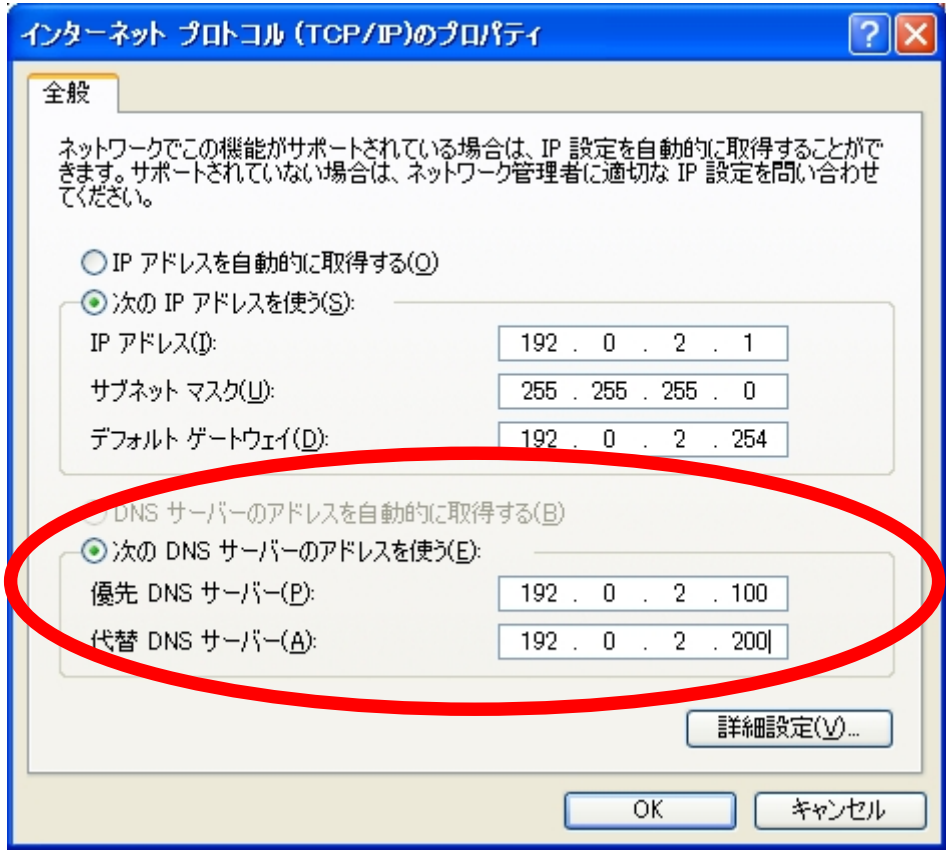
注意点②:
二種類のDNSサーバーの存在

- DNSサービスを提供するサーバーが、二種類ある
  - 「キャッシュDNSサーバー」と「権威DNSサーバー」
- これらのサーバーは機能、サービス対象、サービス提供範囲が異なっているが、いずれも「DNSサーバー」と呼ばれている

それぞれの役割を把握することが重要

どちらの「DNSサーバー」を指しているかについて意識する必要がある

（例）どちらのDNSサーバーを指している？



例1：WindowsのTCP/IPのプロパティ
（キャッシュDNSサーバー）

例2：TechNet「DNSサーバーを計画する」
（権威DNSサーバー）

二種類のDNSサーバーの違い（まとめ）

	キャッシュ DNSサーバー	権威 DNSサーバー
機能	階層構造をたどり 名前解決を実行する	階層構造を構成し 名前情報を管理する
サービス対象	ISPや組織などの ユーザー （DNSクライアント）	インターネット上の キャッシュ DNSサーバー
サービス提供範囲	対象ユーザー （DNSクライアント）のみ	インターネット 全体

注意点③:
二種類の問い合わせの存在

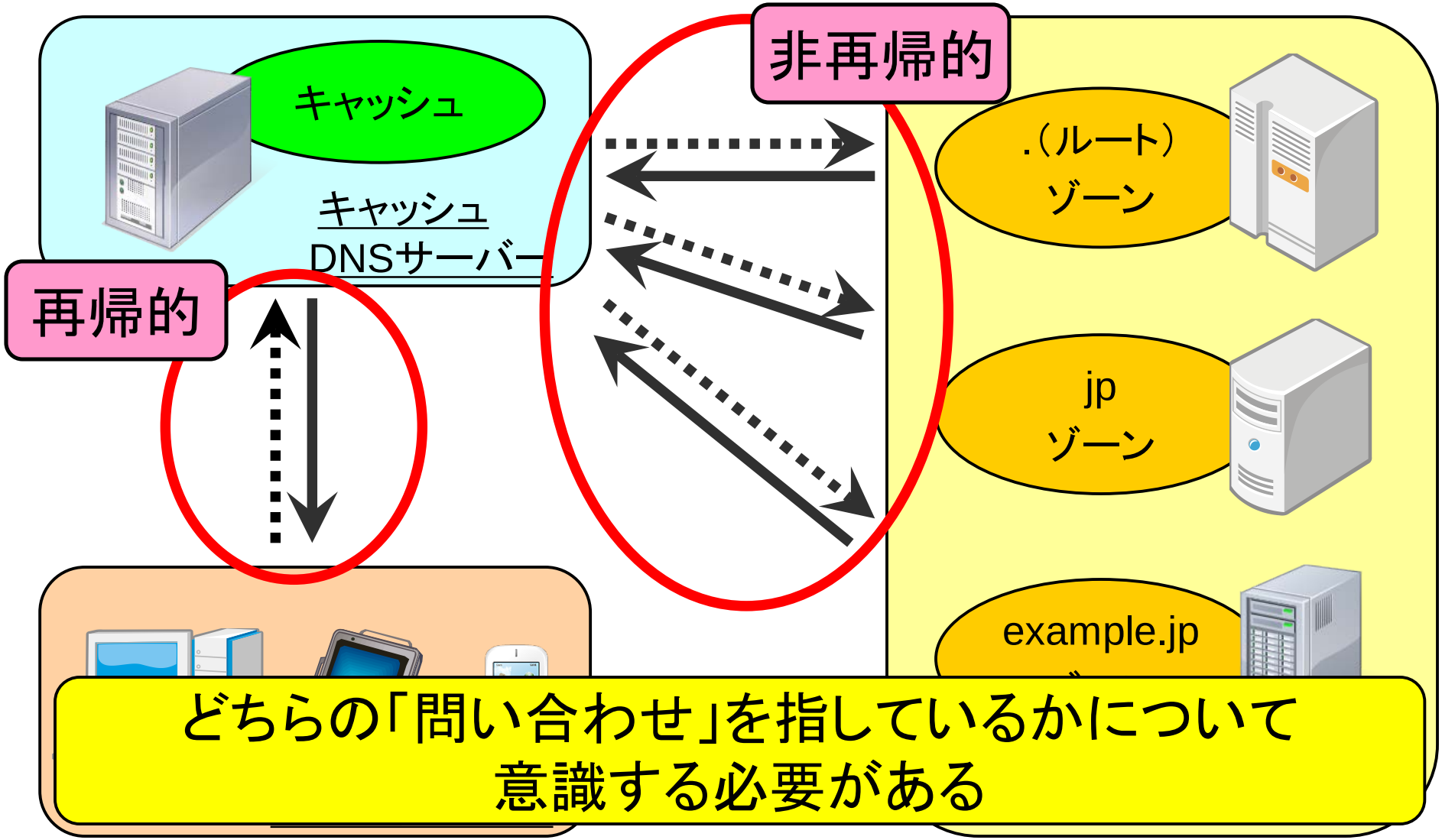
- DNSには、役割の異なる二種類の「問い合わせ」がある
  - 「再帰的問い合わせ」と「非再帰的問い合わせ」
- これらの問い合わせは機能・動作が異なっており、明確に区別する必要がある

次スライドで、役割の違いを説明します

再帰的／非再帰的問い合わせ

- 再帰的問い合わせ（recursive query）
  - 機能：名前解決の依頼（要求）
  - DNSクライアントがキャッシュDNSサーバーに対し、必要に応じて（能動的に）実行
- 非再帰的問い合わせ（non-recursive query）
  - 機能：名前解決の実行
  - 再帰的問い合わせを受信したキャッシュDNSサーバーが、各権威DNSサーバーに対し反復的に実行
    - いわゆる「ツリー構造をたどる」問い合わせ
  - そのため、非再帰的問い合わせは反復問い合わせ（iterative query）とも呼ばれる

再帰的／非再帰的問い合わせ（図解）



どちらの「問い合わせ」を指しているかについて
意識する必要がある

二種類の問い合わせの見分け方

- パケットフォーマット、ポート番号が同一
  - 誤解を生む（理解を妨げる）原因となりうる
  - 特に、キャッシュDNSサーバーと権威DNSサーバーを兼用している場合（後述）、特に誤解を生みやすい
- 見分け方：問い合わせにRDフラグがセットされているか
  - RD=1（セット）：再帰的問い合わせであることを示す
  - RD=0（クリア）：非再帰的問い合わせであることを示す
- RDフラグの意味
  - RD＝Recursion Desiredの略
  - 問い合わせ先に対して、名前解決を要求（Desire）する。

digコマンドで二種類の問い合わせを実施

- 再帰的問い合わせ
  - 問い合わせ先がキャッシュDNSサーバーである場合に使用
  - digコマンドを、オプションを付けずに実行する

  ＜実行例＞dig www.jprs.jp a @8.8.8.8
- 非再帰的問い合わせ（反復問い合わせ）
  - 問い合わせ先が権威DNSサーバーである場合に使用
  - digコマンドに、+norecオプションを付けて実行する

  ＜実行例＞dig +norec www.jprs.jp a @a.dns.jp

二種類の問い合わせの違い（まとめ）

	再帰的問い合わせ	非再帰的問い合わせ （反復問い合わせ）
機能	名前解決を 依頼（要求）する	名前解決を実行する
RDフラグ	RD=1（セット）	RD=0（クリア）
問い合わせ元	DNSクライアント	キャッシュDNSサーバー
問い合わせ先	キャッシュDNSサーバー	権威DNSサーバー
実行形態	必要に応じて 能動的に実行	再帰的問い合わせを 受けて実行
digオプション	デフォルト（+rec）	+norec

注意点④:
兼用可能な実装の存在

- キャッシュDNSサーバーと権威DNSサーバーを一つのプログラムで兼用可能な実装（BIND 9）が存在している
- かつ、BIND 9はデフォルトで双方の機能が有効
  - 双方の機能が兼用されている場合がある
  - 兼用していなくても、双方の機能が有効になって（しまって）いる場合がある

運用上のトラブルを起こさない為に、
機能分離及び適切な機能制限を強く推奨

機能分離・制限を推奨する理由

- DNSの動作・各構成要素の理解促進
- セキュリティ上のリスクの回避
  - オープンリゾルバーになりやすい
  - DNSキャッシュポイズニング攻撃を受けやすい
- 機能干渉の防止
  - 障害発生時の切り分け
- 設定・運用コストの軽減・トラブルの防止
- 将来の移行を考慮
  - BIND以外の多くの実装では双方の機能は分離されている
  - BIND 9の開発元のISCも分離を推奨している

ここまでのまとめ

- DNSの基本構成要素とそれぞれの役割
  - DNSクライアント：名前解決を依頼
  - キャッシュDNSサーバー：名前を検索
  - 権威DNSサーバー：名前を管理
- DNSを理解・運用するにあたっての注意点

① 基本要素に関する名称の不統一
  - どの構成要素を指しているか

② 異なる二種類のDNSサーバー
  - キャッシュDNSサーバーと権威DNSサーバー

③ 異なる二種類の問い合わせ
  - 再帰的問い合わせと非再帰的問い合わせ

④ 兼用可能な実装の存在
  - キャッシュDNSサーバーと権威DNSサーバーの分離を強く推奨

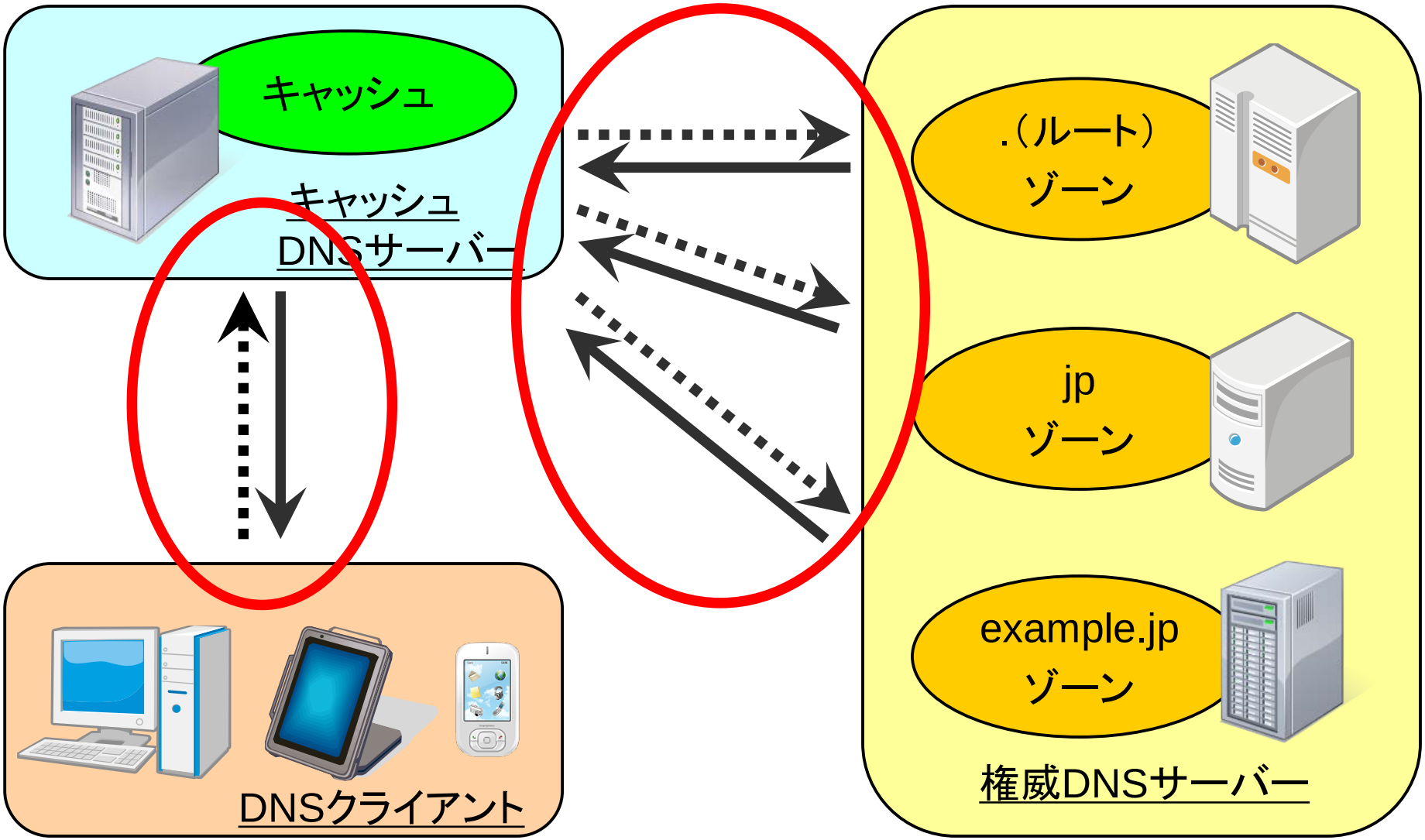
2. DNSにおけるIPv6対応
～理論編～

二つの独立した「IPv6対応」

- DNSには二つの「IPv6対応」が存在する
  - DNS通信におけるIPv6対応
    - DNSの通信をIPv6に対応させる
  - DNSリソースレコード（RR）におけるIPv6対応
    - DNSの登録情報をIPv6に対応させる

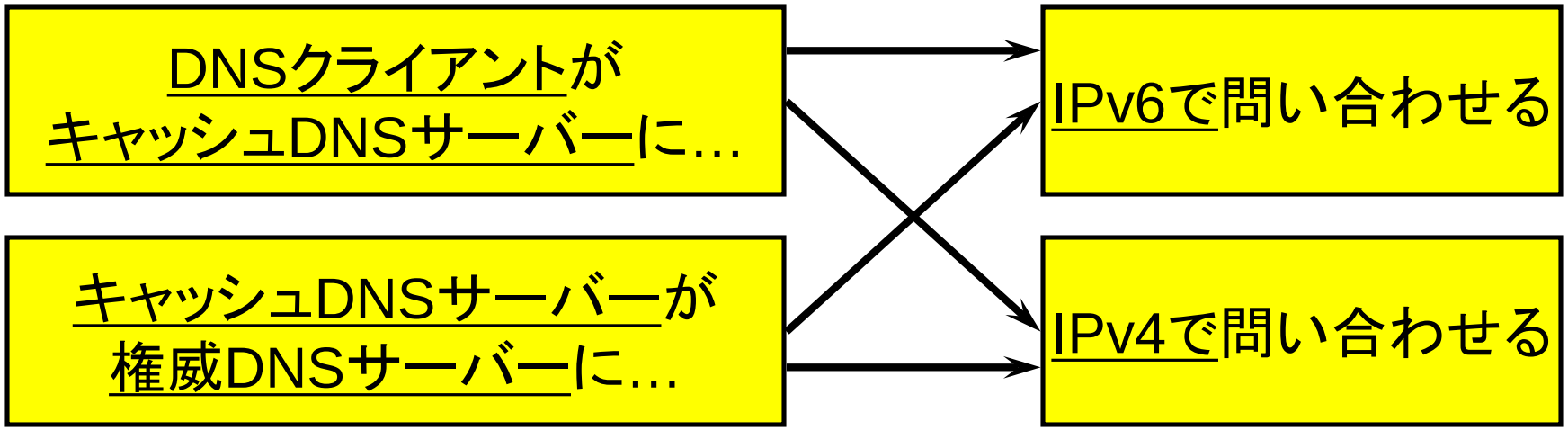
これらは互いに独立していることに注意

考慮点①：DNS通信におけるIPv6対応



DNS通信におけるIPv6対応

- 基本構成要素を個別にIPv6対応する必要がある
  - DNSクライアント
  - キャッシュDNSサーバー
  - 権威DNSサーバー
- それぞれの通信は独立であることに注意



DNS通信におけるIPv6対応 ～DNSクライアント編～

- IPv6でDNS問い合わせを送信できるようにする
  - クライアントにIPv6アドレスが設定される
  - DNS問い合わせを発行するライブラリー（スタブリゾルバー）が、IPv6での問い合わせに対応する
- クライアントがIPv6を送信できない例
  - Windows XPではクライアントにIPv6アドレスを設定できるが、DNSライブラリー（スタブリゾルバー）がIPv6での問い合わせに対応していないため、IPv6でのDNS通信は実行されない

DNS通信におけるIPv6対応 ～キャッシュDNSサーバー編①～

- 二つの対応を考慮する必要あり
  - DNSクライアントからの再帰問い合わせを、IPv6で受信できるようにする
  - 権威DNSサーバーへの非再帰（反復）問い合わせを、IPv6で送信できるようにする
- BIND 9やUnboundなど最近のキャッシュDNSサーバーの実装では、いずれにも対応済

DNS通信におけるIPv6対応 ～キャッシュDNSサーバー編②～

- 現状において（かつ当分の間）、インターネット上の権威DNSサーバーはIPv4でサービスされる
  - そのため、キャッシュDNSサーバーはIPv6/IPv4の双方で非再帰問い合わせを送信できる必要がある
  - つまり、デュアルスタックが必須（RFC 3901で規定）
- DNSクライアントからの問い合わせの受信については、運用形態によりIPv6シングルスタックにすることも可能
  - DNS64（後述）の利用など

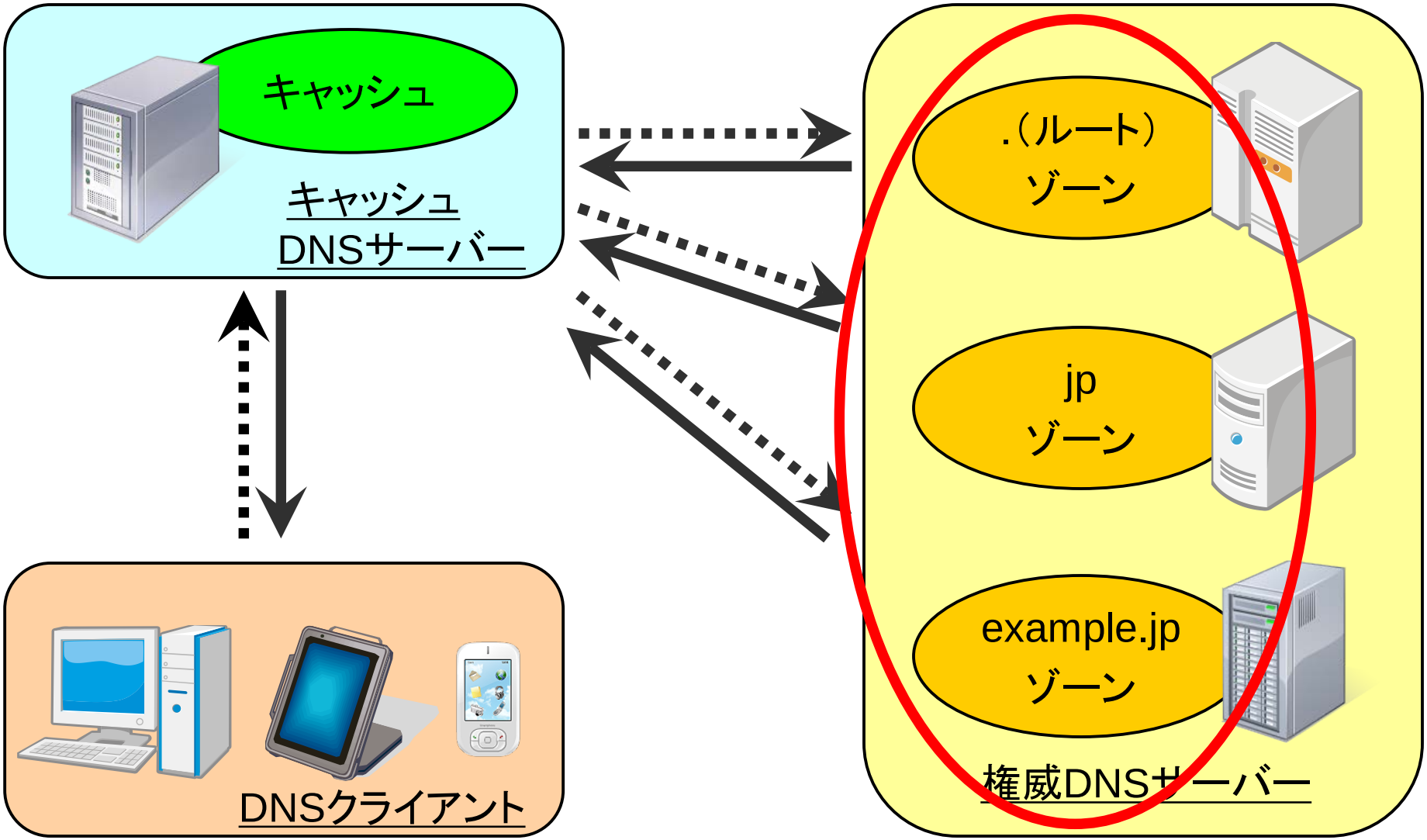
DNS通信におけるIPv6対応 ～権威DNSサーバー編①～

- IPv6、IPv4の双方でDNSデータを公開
- BIND 9やNSDなど最近の権威DNSサーバーの実装では、IPv6でのサービスに対応済

DNS通信におけるIPv6対応 ～権威DNSサーバー編②～

- IPv6とIPv4で同じDNSデータを提供することが必須（RFC 4472で規定）
- 同じDNSデータを提供していれば、IPv6とIPv4の権威DNSサーバーを別にすることも可能
  - 別にする場合、データの同期に注意する必要あり
- 同じサーバーを用い、デュアルスタックで運用することも当然可能

考慮点②：DNS RRにおけるIPv6対応



DNS RRにおけるIPv6対応

- IPv6に関係するDNS RR
  - AAAA（クワッド・エー）レコード（正引き）
  - PTR（ポインター）レコード（逆引き）

AAAAレコードの基本

- あるホスト名に対応するIPv6アドレスを記述
- 名前の由来
  - IPv4アドレス（32ビット）を記述するAレコードに対し、4倍（128ビット）の長さを持つため
- AAAAレコードの記述例

```
$ORIGIN example.jp.
example.jp.   IN     SOA    …
www.example.jp.      IN     A      192.0.2.1
www.example.jp.      IN     AAAA   2001:db8::1
```

- BIND 9やNSDなど最近の権威DNSサーバーの実装では、AAAAの記述を標準でサポートしている

権威DNSサーバー自身のIPv6アドレスの指定（1/3）

- DNSでは以下の二つの情報の組み合わせで、各権威DNSサーバーを指定

  ①権威DNSサーバーのホスト名（NSレコード）
  ②そのホスト名のIPアドレス（Aレコード）

- 権威DNSサーバー自身のIPアドレスの情報も、DNSの登録情報として管理
  - DNS RR（Aレコード）で指定

```
$ORIGIN example.jp.
@                       IN      SOA     …
                        IN      NS      ns1.example.jp.
ns1                     IN      A       192.0.2.101
```

権威DNSサーバー自身のIPv6アドレスの指定（2/3）

- そのため、権威DNSサーバーをIPv6対応する場合、そのホスト名のIPv6アドレスも併せて指定する必要がある
  - Aレコードに加え、AAAAレコードを併せて指定

```
$ORIGIN example.jp.
@                       IN      SOA     …
                        IN      NS      ns1.example.jp.
ns1                     IN      A       192.0.2.101
ns1                     IN      AAAA    2001:db8::101
```

権威DNSサーバー自身のIPv6アドレスの指定(3/3)

- そして、この情報(ネームサーバーホスト情報)を、自分の親ゾーンに登録する必要がある
  - ホスト名(NSレコード)
  - IPv4アドレス(Aレコード)
  - IPv6アドレス(AAAAレコード)
- そのため、レジストリやレジストラなどの登録システムにおいて、IPv6アドレスの登録をサポートしている必要がある
  - JPドメイン名においては、JPRSはレジストリとして、IPv6アドレスの登録をサポート済

PTRレコードの基本

- あるIPv6アドレスに対応するホスト名を記述
  - いわゆる「逆引き」
- PTRレコードを用い、アドレスを逆順で記述するという点ではIPv4と場合と同じ
- ただし、IPv4のPTRレコードとは区切りのビット数と使用するドメイン名が異なっている

	IPv4	IPv6
区切りのビット数	8ビットごと	4ビットごと
使用ドメイン名	in-addr.arpa	ip6.arpa

PTRレコード記述時の注意

- PTRレコードの記述例（実際には一行で記述）

```
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1
.0.0.2.ip6.arpa.    IN     PTR    www.example.jp.
```

- 長いので桁数を間違えないように注意
- 間違えないためのTips
  - $ORIGINディレクティブを適宜使用する
  - digの-xオプションやarpanameコマンドを使用する

```
$ dig -x 2001:db8::1
$ arpaname 2001:db8::1
```

BIND 9.7以降に標準添付

PTRレコードの設定方法と現状

- PTRレコードの設定には、二通りの方法がある
  - 管理するISPなどに依頼する
  - 管理するISPなどから当該逆引きゾーン（/48や/64）単位での委任を受ける
- IPv6における逆引きサービスを提供していない事業者が存在する
  - 特にユーザーのアクセス回線はほぼ設定なし
- ただし、2013年8月の「GmailにおけるIPv6逆引きの必須化（後述）」により、今後逆引き設定が促進されていく可能性もある

ここまでのまとめ

- DNSには二つの「IPv6対応」が存在する
  - DNS通信におけるIPv6対応
  - DNSリソースレコード（RR）におけるIPv6対応
- DNS通信におけるIPv6対応
  - 三つの基本構成要素を個別にIPv6対応する必要がある
    - DNSクライアント、キャッシュDNSサーバー、権威DNSサーバー
  - キャッシュDNSサーバーはデュアルスタック必須
  - 権威DNSサーバーはIPv6/IPv4別々でも良い
    - ただし、IPv6/IPv4で同一のデータの提供が必須
- DNS RRにおけるIPv6対応
  - AAAAレコード（正引き）とPTRレコード（逆引き）
  - サーバーのほか、登録システムにおいても対応が必要
  - PTRレコード記述の際にはdig –x/arpanameコマンドが便利

3. DNSにおけるIPv6対応
～実践編～

構成要素ごとに考慮する必要あり

① DNSクライアントにおける対応
② キャッシュDNSサーバーにおける対応
③ 権威DNSサーバーにおける対応

①DNSクライアントにおけるIPv6対応

- DNSクライアントがIPv6でDNS問い合わせを送信できるようにする
  - クライアントにIPv6アドレスが設定（配布）される
  - DNS問い合わせを発行するライブラリー（スタブリゾルバー）が、IPv6での問い合わせに対応する

クライアントへのIPv6アドレスの設定

- DNSクライアントとキャッシュDNSサーバー間の通信におけるIPv6対応は、組織やISPがユーザーにどのようにIPv6サービスを提供するかにより、戦略が異なる
- クライアントへのIPv6アドレス設定（配布）方法
  - RA※1（SLAAC※2） or DHCPv6
  - PPPoE
- DNSの観点から見たRA（SLAAC）とDHCPv6
  - RA（SLAAC）
    - 従来のRAはキャッシュDNSサーバーの情報を設定不可能
    - RFC 6106でRAのオプションが拡張され、設定可能に
  - DHCPv6
    - キャッシュDNSサーバーの情報を設定可能

※1 RA=Router Advertisement

※2 SLAAC=Stateless Address Auto Configuration

デュアルスタック or シングルスタック

- ユーザーにどの形でサービスを提供するか
  - IPv6/IPv4デュアルスタック
  - IPv6シングルスタック（+NAT64/DNS64）
- それぞれにメリット・デメリットが存在

DNS64の概要については後述

IPv6/IPv4デュアルスタック

- ユーザーに従来のIPv4に加え、IPv6も提供
- IPv6/IPv4いずれのサービスにも接続可能
- デュアルスタック構成だと、ユーザー側で利用するネットワークを選択する必要が生じる
  - エンドポイントの動作が複雑になる
- デュアルスタック化に起因する問題が発生しうる
  - フォールバック問題（後述）など

IPv6シングルスタック+NAT64/DNS64

- ユーザーにはIPv6のみを提供し、IPv4にはNAT64/DNS64で対応
- シングルスタック構成だと、ユーザー側でネットワークを選択する必要が生じない
  - エンドポイントの動作をシンプルにできる
- デュアルスタック化に起因する問題を回避可能
- クライアントの種類やサービスが限定されている場合など、有効なサービス提供手段となりうる
  - 例：携帯電話の網内ネットワークなど
- 一部、対応できないケースが存在する（後述）

②キャッシュDNSサーバーにおける対応

- IPv6/IPv4のデュアルスタック構成となる
- IPv6においてもIPv4と同様、適切なアクセスコントロールや機能制限を実施する必要がある
  - IPv6対応に応じた設定追加を忘れがちなので注意
  - 特に、オープンリゾルバーにならないように
- BIND 9の場合、named.confにおける設定内容に以下の二種類が存在することに注意
  - IPv4/IPv6アドレスを併記するもの
  - IPv6アドレス用のオプションがあるもの

次スライドで、二種類の設定内容について説明する

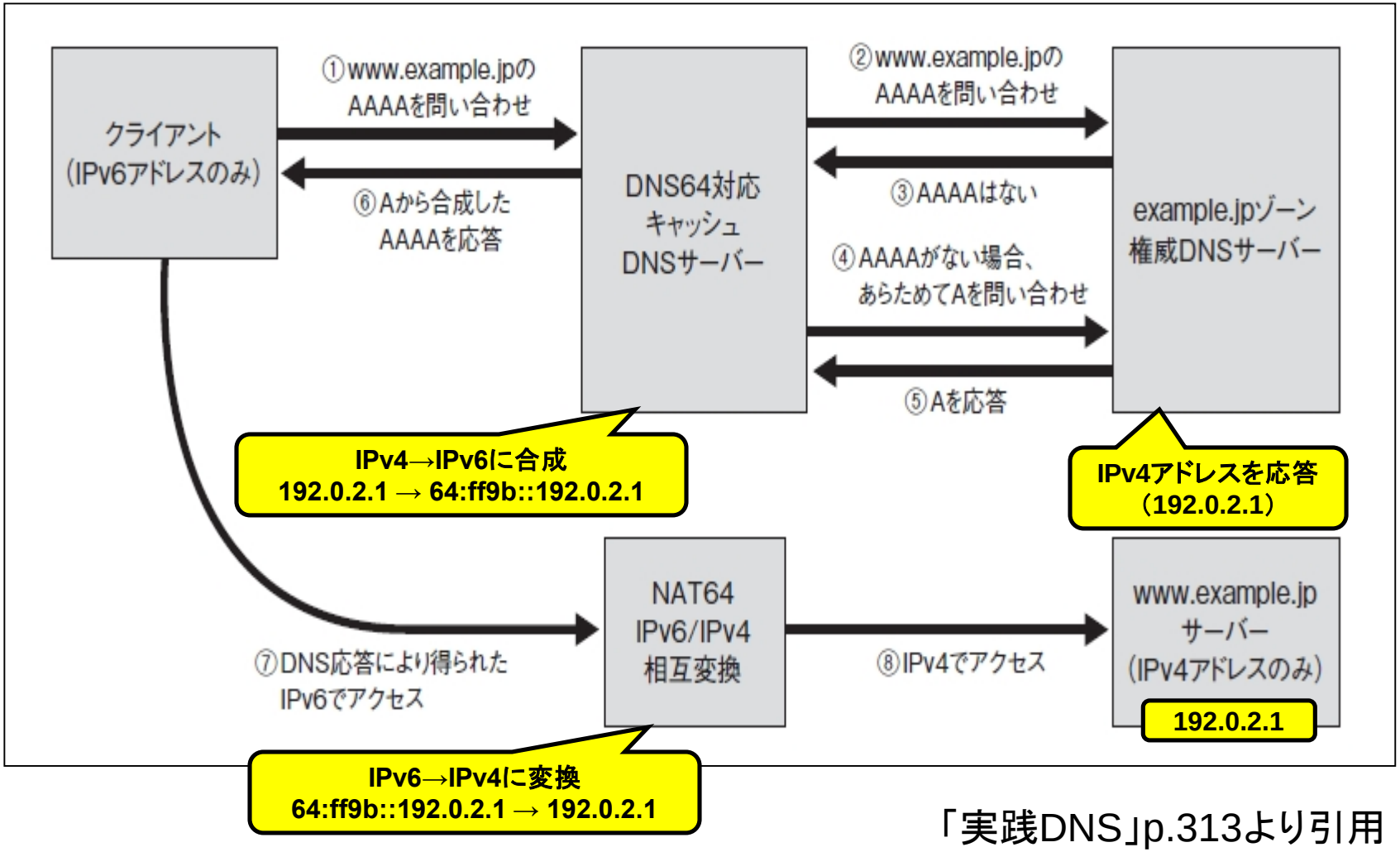
BIND 9における二種類のオプション

- IPv4/IPv6アドレスを併記するもの
  - allow系
    - allow-query, allow-recursion, allow-query-cache, allow-notify, allow-transfer, など
  - match系
    - match-destinations, match-clients, など
  - zoneステートメント内のmasters
- IPv6専用のオプションがあるもの
  - listen-on-v6（listen-on に対応）
  - query-source-v6（query-source に対応）

キャッシュDNSサーバーにおけるDNS64の概要

- IPv6アドレスのみのクライアントからIPv4アドレスのみのサーバーへの接続を実現するための技術
- RFC 6147で定義、NAT64（RFC 6146）との併用が前提
- クライアントからのAAAAレコードの問い合わせに対し、NAT64で変換されたIPv6アドレスを返すようにキャッシュDNSサーバーで設定
- これによりNAT64で変換された接続先に、ドメイン名を用いて接続することが可能になる

NAT64/DNS64による接続の流れ



「実践DNS」p.313より引用

NAT64/DNS64の限界

- NAT64ではうまく対応できないサービスの存在
  - Dropbox、Skypeなどプロプライエタリーなサービスの一部
  - IPv6／v4トランスレーターの実装にも依存
- DNS64がうまく動作しないケースの存在
  - 生のIPv4アドレスを直接指定しているサービス（DNS問い合わせをしない）には対応不可
  - RFC 4074にある誤った動作（misbehavior）をするネットワーク機器
    - AAAAレコードの問い合わせに対し異常な応答を返す
    - 特定のロードバランサーなど

BIND 9におけるDNS64の設定例

```
options {
        dns64 64:ff9b::/96 {
                clients {// DNS64を適用したいIPv6クライアント
                        2001:db8:1:1::/64;
                };
                exclude {// 上記の内、適用除外したいIPv6クライアント
                        2001:db8:1:1::20/128;
                };
                mapped {// DNS64を適用する、IPv4アドレスをマップ
                        !192.168.0.0/16;
                        any;
                };
                // 再帰問い合わせにのみ適用
                recursive-only yes;
        };
};
```

③権威DNSサーバーにおける対応

- キャッシュDNSサーバーと同様にIPv6においても、適切なアクセスコントロールや機能制限を実施する必要がある
- デュアルスタック（同一サーバー）とするか、IPv6とIPv4のサーバーを別にするかを考慮・決定する必要がある
  - 権威DNSサーバーはいずれの構成でも運用可能
  - 各組織/ISPにおけるサーバー構成戦略や運用ポリシーにより異なる

IPv4のみの権威DNSサーバー

- JP DNSでは、2008年にIPv4のみをサービスするDNSサーバー（g.dns.jp）を追加

> JP DNSなどの権威サーバですべてのDNSサーバがIPv4/IPv6のデュアルスタックになると、キャッシュサーバの実装とそのネットワーク環境によっては不具合がおきることがあるという報告があります。これについての詳細は未確認ですが、JP DNSでは、運用面の安全性を考慮し当面の間IPv4だけのサーバを維持する方針で運用するため、新たにg.dns.jpをIPv4のみのサーバとして追加します。
>
> JP DNSサーバの構成について - 2008年10月版 - <http://jprs.jp/tech/jp-dns-info/2008-10-06-jp-dns-servers.html>より引用

- 最近では、すべての権威DNSサーバーにIPv6/IPv4アドレスが付与されているドメイン名も数多く存在している
- JP DNSでは安全性を最大限に考慮し、今後もIPv4のみの権威DNSサーバーの運用を継続する予定

ここまでのまとめ

- DNSクライアントにおける対応
  - 組織やISPがユーザーにどのようにIPv6サービスを提供するか
  - クライアントへのIPv6アドレス設定（配布）方法
    - RA（SLAAC） or DHCPv6
  - デュアルスタックかシングルスタックか
- キャッシュDNSサーバーにおける対応
  - IPv6/IPv4のデュアルスタック必須
  - IPv4と同様、適切なアクセスコントロールや機能制限が必須
  - BIND 9の場合、named.confにおける設定内容の種類に注意
  - NAT64/DNS64の概要と設定例
- 権威DNSサーバーにおける対応
  - IPv4と同様、適切なアクセスコントロールや機能制限が必須
  - IPv6/IPv4を同一サーバーとするか別にするかを考慮・決定する必要あり
  - JP DNSでは安全性のため、IPv4のみの権威DNSサーバーを運用中

4. DNS/IPv6関連トピックス

①AAAAフィルターの概要と注意点
②GmailにおけるIPv6逆引きの必須化

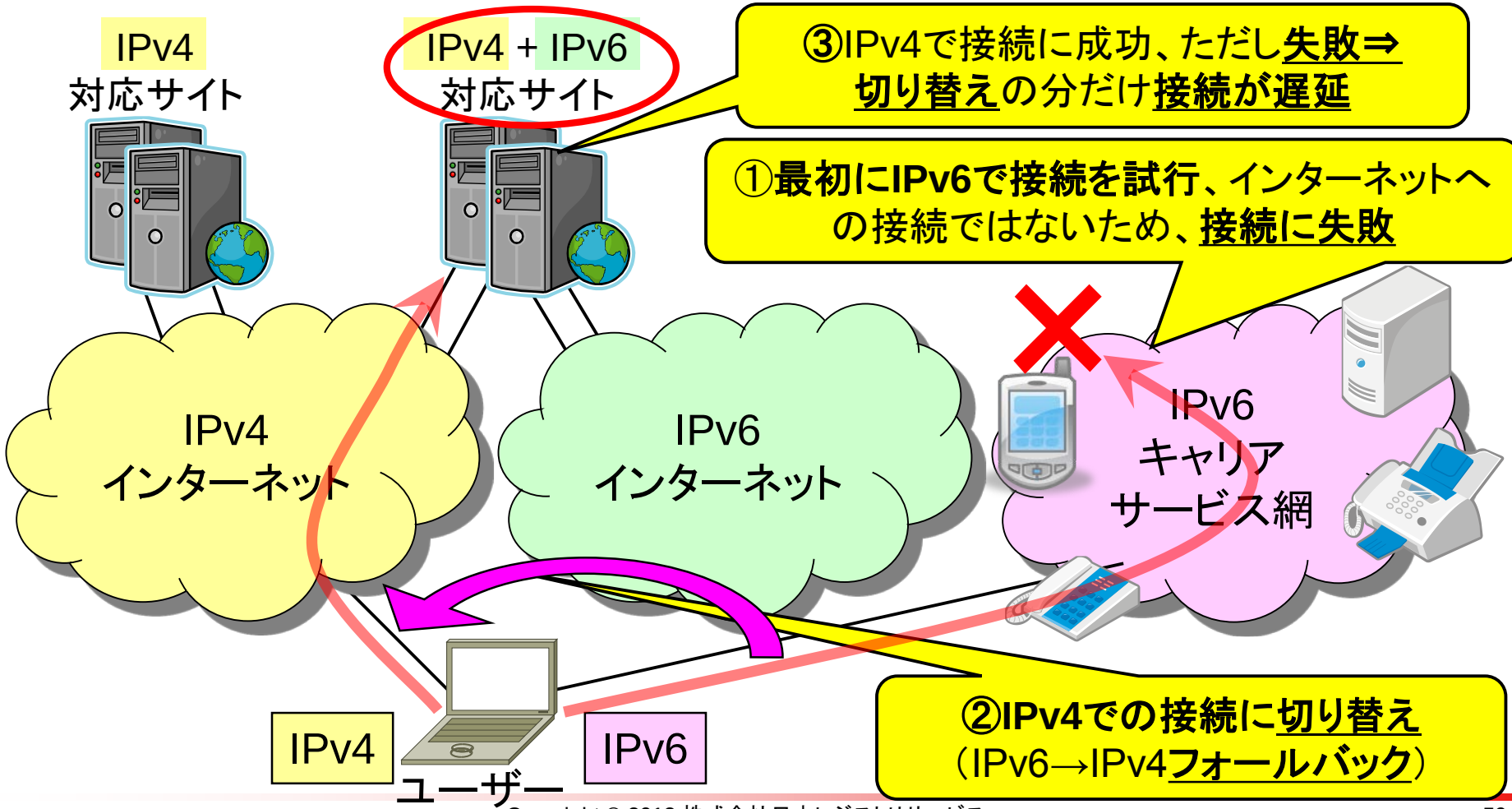
トピックス①:
AAAAフィルターの概要と注意点

- IPv6→IPv4フォールバック問題を一時的に回避するために導入された対策
  - ユーザーにIPv6を利用させないようにする
- 本来すべき対策は「問題の根本的な解決」
  - ユーザーのIPv6アクセスが失敗しないようにする
    →IPv6インターネット接続の実現

IPv6→IPv4フォールバック問題とは何だったのか？

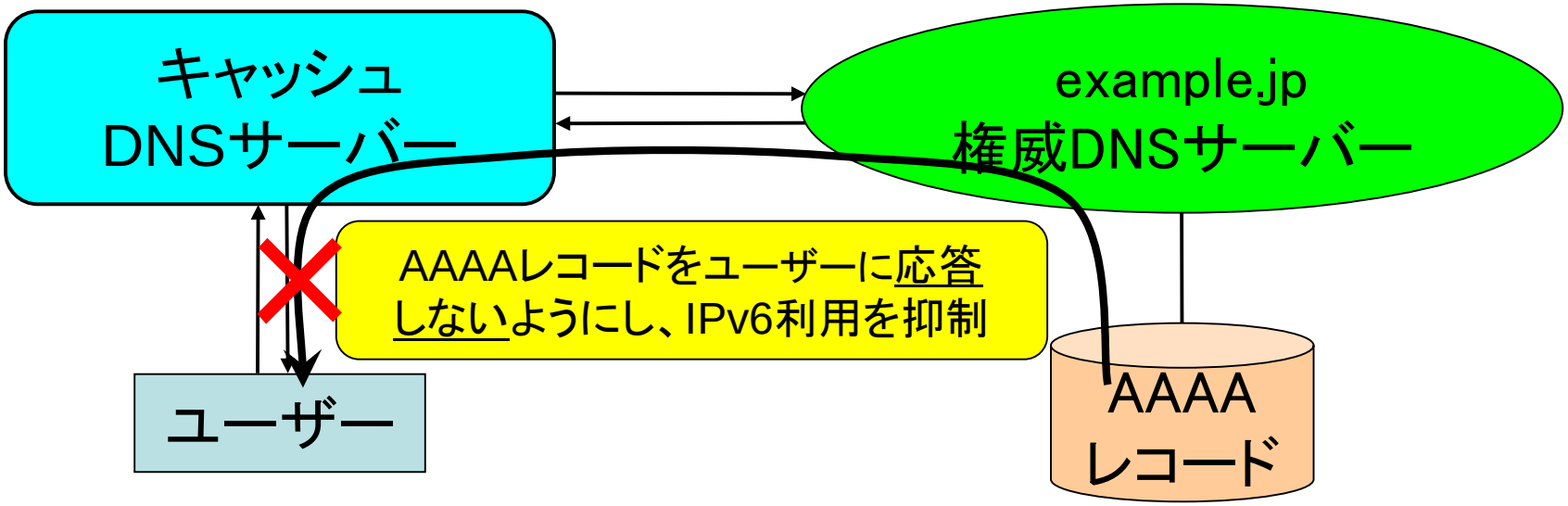
IPv6→IPv4フォールバック問題

「IPv4インターネット」と「IPv6キャリアサービス網」に接続しているユーザーが「IPv4+IPv6対応サイト」を使う場合に問題となる



AAAAフィルターとは？

- DNSを用いたフィルタリングの一種
- 何らかの手法によりユーザー（クライアント）に対し、AAAAレコードを応答しないようにする
  - 「そのサイトはIPv6サービスを提供していない」と判断させる
- ユーザーのIPv6利用を抑制するための手段の一つ

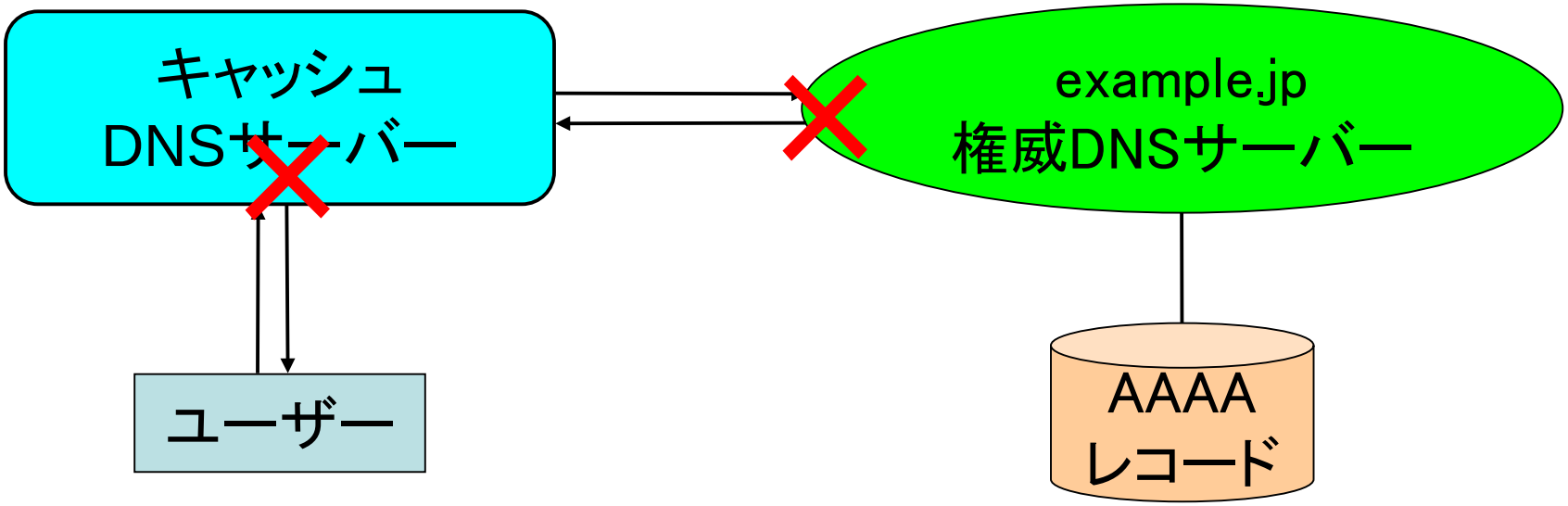


AAAAフィルターの目的と背景

- IPv6を利用させないように誘導することで、IPv6の利用によりユーザーが遭遇しうる不具合を回避する
- 導入検討の前提条件
  1）ユーザーがIPv6の利用を試みる可能性がある
  2）かつ、ユーザーがIPv6を利用しようとした場合、何らかの不具合が発生する可能性が高い
- World IPv6 Launch（2012年6月6日）に伴い、問題の回避策の一つとして複数ISPが導入

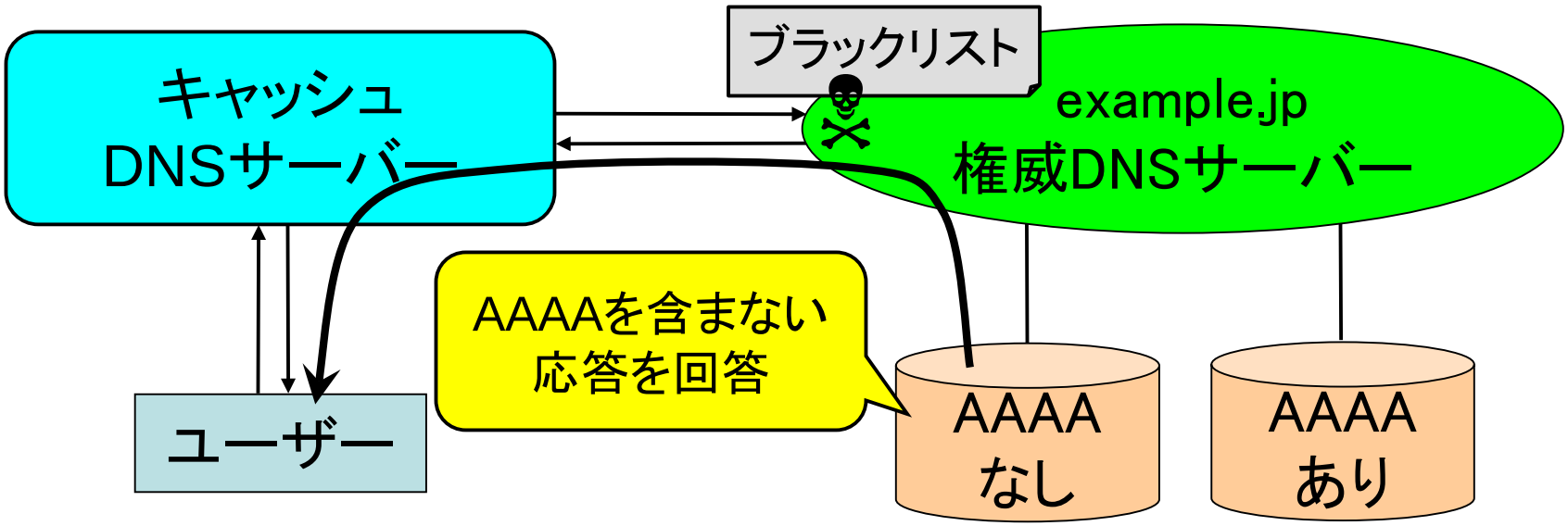
二種類の「AAAAフィルター」

- 誰がAAAAフィルターを設定するかにより分類
- 権威DNSサーバーにおけるAAAAフィルター
  - キャッシュDNSサーバーにAAAAを応答しない
- キャッシュDNSサーバーにおけるAAAAフィルター
  - ユーザーにAAAAを応答しない



権威DNSサーバーにおけるAAAAフィルター

- ブラックリスト方式により特定のIPアドレス（キャッシュDNSサーバー）からの問い合わせに対し、AAAAを含まない応答を回答
- World IPv6 Launchに際し、Google、Facebookを始めとする米国の大手コンテンツプロバイダーが導入
- Googleが公開しているブラックリスト（現在も更新中）
  - http://www.google.com/intl/en_ALL/ipv6/statistics/data/no_aaaa.txt

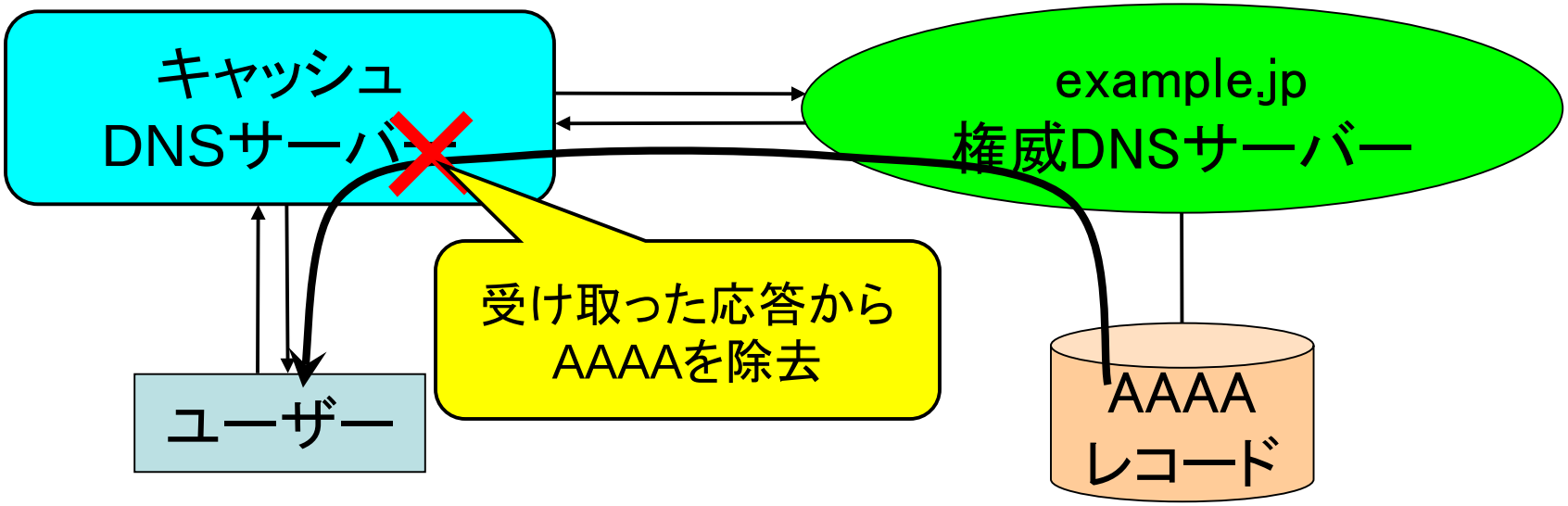


この手法の特徴

- DNSSECに対応可能
  - 通信途中で応答を書き換えているわけではないため
  - デュアルスタックのキャッシュDNSサーバーでは、DNSSEC検証に失敗する可能性あり
    - AAAAありとAAAAなしのNSEC/NSEC3を受け取る可能性がある
- きめ細かな制御が難しい
  - 当該キャッシュDNSサーバーのすべてのユーザーに対し、AAAAフィルターが適用されてしまう
- フィルター解除はコンテンツプロバイダーが実施
  - 当該キャッシュDNSサーバーのすべてのユーザーに影響がないと当該コンテンツプロバイダーが判断するまで、AAAAフィルターが適用され続ける

キャッシュDNSサーバーにおけるAAAAフィルター

- キャッシュDNSサーバーが権威DNSサーバーから受け取った応答から、AAAAレコードを除去
- 「AAAAフィルター」と言った場合、通常はこの手法を指す
  - 以降の本資料における「AAAAフィルター」もこちらを指す
- World IPv6 Launchに伴い複数ISPが導入



この手法の特徴(1/2)

- きめ細かな制御が可能
  - ISPのユーザーごと／IPアドレスごとにAAAAフィルターの有効・無効の制御が可能
- DNSSECには対応不可能
  - 通信途中でデータを書き換えた場合、DNSSECによる検証が不可能になる

この手法の特徴(2/2)

- 応答作成のコストが高い
  - DNSプロトコルに合致した応答を作成する必要あり
  - 単なるAAAAレコードの除去だけでは不十分
  - これによる副作用については後述
- フィルター解除はISPが実施
  - ISPがキャッシュDNSサーバーを顧客に提供する場合が多いため、IPv6によるインターネット接続を顧客に提供した時点でAAAAフィルターを解除する、といった運用が可能になる

BIND 9における AAAAフィルターの実装（1/2）

- BIND 9.7以降で実装
- BINDのコンパイル（configure）において、
  - `--enable-filter-aaaa`を明示的に指定し、（デフォルトでは機能そのものが組み込まれない）
- かつ、設定（named.conf）において、
  - `filter-aaaa-on-v4`オプションに`yes`または`break-dnssec`オプションを指定した場合にのみ、AAAAフィルターが有効になる
  - デフォルトでは**no**（AAAAフィルター無効）

BIND 9における AAAAフィルターの実装(2/2)

- BINDのマニュアル(ARM)に以下の記述がある
  - “This is not recommended unless absolutely necessary.”「訳:これは絶対に必要でない限り推奨されない。」

AAAAフィルターはあくまでも、他の方法では障害発生が不可避な場合の非常手段という位置づけ

「yes」と「break-dnssec」の違い（1/3）

- filter-aaaa-on-v4で設定可能な内容（3種類）
  - filter-aaaa-on-v4 (yes | no | break-dnssec);

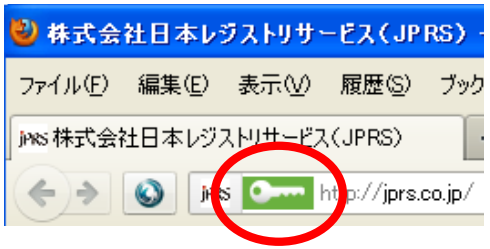
「yes」と「break-dnssec」はどう違うのか？

➢「yes」：AAAAフィルター有効、ただし…
  - IPv6による問い合わせに対しては自動的に無効
    - IPv6で問い合わせを出せる≒IPv6でアクセスできる
  - IPv6でキャッシュDNSを提供しているISPのユーザーがIPv6を利用しても、不具合は発生しない**はず**、という考え方に基づいている

「yes」と「break-dnssec」の違い（2/3）

- 「yes」：AAAAフィルター有効、ただし…（続き）
  - 応答がDNSSEC署名つき（=DNSSEC対応したドメイン名）であった場合、自動的に無効
  - キャッシュDNSサーバーでDNSSEC検証を有効にしていない場合も無効になるので注意

- 理由：クライアント（アプリケーション）におけるDNSSEC検証を妨げないため
- 既存のアプリケーション例
  - CZ.NICによるWebブラウザー用DNSSEC Validator
  - DNSSEC authenticated HTTPS in Google Chrome



「yes」と「break-dnssec」の違い（3/3）

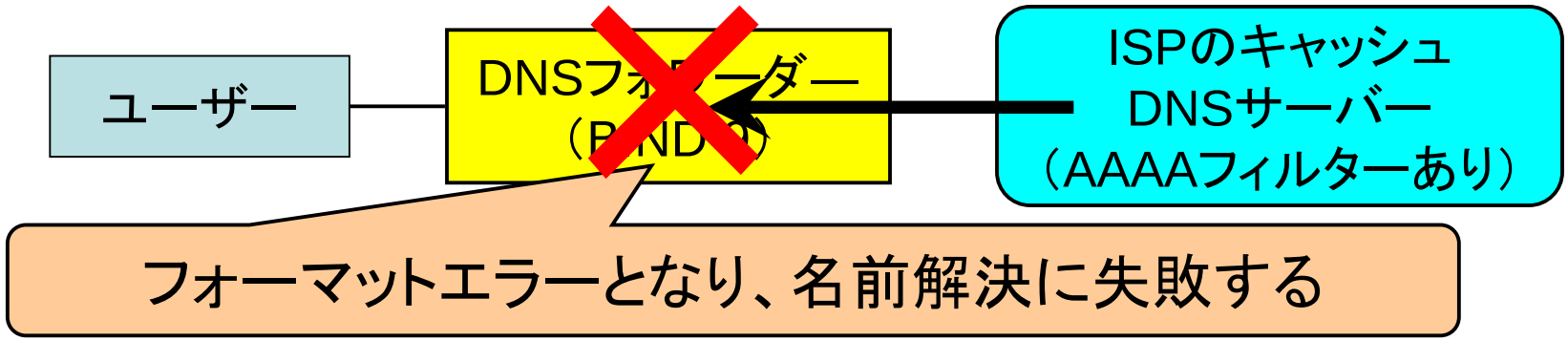
- 「break-dnssec」:「yes」に加え、DNSSEC署名つきの応答であってもAAAAフィルターを強制的に有効に設定
- 導入による副作用
  - クライアント（アプリケーション）におけるDNSSEC検証ができなくなる（失敗する）
  - 前述したアプリケーションが正しく動かなくなる

AAAAフィルターにおける注意事項(1/2)

- キャッシュDNSサーバーにおけるAAAAフィルターでは、DNSプロトコルに(厳密に)違反しない応答の合成(synthesis)に手間(コスト)がかかる
  - BIND 9における現在の実装は不完全
  - 作成にかかるコストが高いため、他の実装も同じ問題を持っている可能性が高い
- 結果として、DNSプロトコル的に壊れた応答がDNSクライアント(スタブリゾルバー)に返される可能性がある
- ただし、応答を受け取るのがDNSクライアントである場合、厳密な応答のチェックがされないため、ほぼ問題にならない

AAAAフィルターにおける注意事項(2/2)

- しかし、応答を受け取るのがDNSフォワーダーやDNSプロキシーであった場合、DNS応答が不正であると判定される場合がある
- 例えば、BIND 9をDNSフォワーダー(type forward)として使用している場合、フォワード先のキャッシュDNSサーバーから送られる応答にAAAAフィルターが適用されていた場合、FORMERR(フォーマットエラー)となり、名前解決に失敗するので注意が必要(下図)



トピックス②:
GmailにおけるIPv6逆引きの必須化

- 2013年8月18日ごろ、Gmailの仕様が予告なく変更（以下の記述がGmailヘルプに追加）された

IPv6 向けの追加のガイドライン

•送信元 IP には PTR レコード（送信元 IP の逆引き DNS）が必要です。また、PTR レコードで指定されているホスト名の DNS の正引き解決によって取得した IP と一致している必要があります。そうでない場合は、メールに迷惑メール マークが付けられたり、メールが拒否されることがあります。
•送信元ドメインは、SPF チェックまたは DKIM チェックにパスする必要があります。そうでない場合は、メールに迷惑メール マークが付けられることがあります。

<https://support.google.com/mail/answer/81126> より引用

何が起きたのか？

- IPv6の場合にのみ、Gmailへの送信元IPアドレスについて、以下の二つの条件を満たすことが必須となった

①逆引き（PTRレコード）が設定されていること
②かつ、逆引きで設定されたホスト名を再び正引きして得られたIPv6アドレスが、送信元IPv6アドレスと一致していること

- 従来、IPv6のアクセス回線における逆引きはほとんど設定されていなかったため、多くのIPv6ユーザーがGmailのアドレスにメールを送信できなくなった
- 一部のユーザーはGmailへの送信時のみIPv4を利用するように設定変更し、障害を回避

この設定内容について

- この設定内容（①逆引きの必須化、②いわゆるパラノイアチェック（逆引き結果を再び正引きして検証））は、IPv4の世界ではインターネットの黎明期から広く用いられている認証手法の一つ
- しかし、IPv6の世界でこの設定を適用する例はこれまでほとんど報告されていなかった
- （2013年10月21日追加）メール送信にSubmission portを使用し、かつSMTP AUTHで認証すれば、IPv6逆引きがなくてもGmailにメールを送信可能
  - MTA（メール転送エージェント）:IPv6逆引きをきちんと記述
  - MSA（メール投稿エージェント）:Submission portかつSMTP AUTH

参考リンク（本資料から参照したDNS関連RFC）

- RFC 3901
  - DNS IPv6 Transport Operational Guidelines（DNSのIPv6トランスポートの運用ガイドライン）
- RFC 4472
  - Operational Considerations and Issues with IPv6 DNS（IPv6 DNSに関する運用上の考慮点と課題）
- RFC 6106
  - IPv6 Router Advertisement Options for DNS Configuration（DNS設定のためのIPv6 RAオプション）
- RFC 6147
  - DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers（DNS64: IPv6クライアントからIPv4サーバーへのネットワークアドレス変換のためのDNS拡張）

参考リンク（AAAAフィルター、Gmail逆引き関連）

- AAAAフィルター関連
  - JAIPAによる公開資料
    - World IPv6 Launch についてのご案内

    <http://www.jaipa.or.jp/ipv6launch/>
  - JPRS民田の発表資料（JANOG29）
    - AAAAフィルタとDNSSECは仲良くなれるのか

    <http://www.janog.gr.jp/meeting/janog29/_downloads/janog29-aaaa-after-minda-01.pdf>
- GmailにおけるIPv6逆引きの必須化関連
  - Googleの公式文書
    - 一括送信ガイドライン - Gmail ヘルプ

    <https://support.google.com/mail/answer/81126>
  - Google グループにおける2013年8月18日の書き込み（設定変更初日）
    - e-mail to gmail.com bouncing with 550-5.7.1 errors

    <http://productforums.google.com/forum/#!topic/gmail/K5klFKDnUAE>

Q&A