Empowered by Innovation NEC

Home Gatewayにまつわる DNS話あれこれ

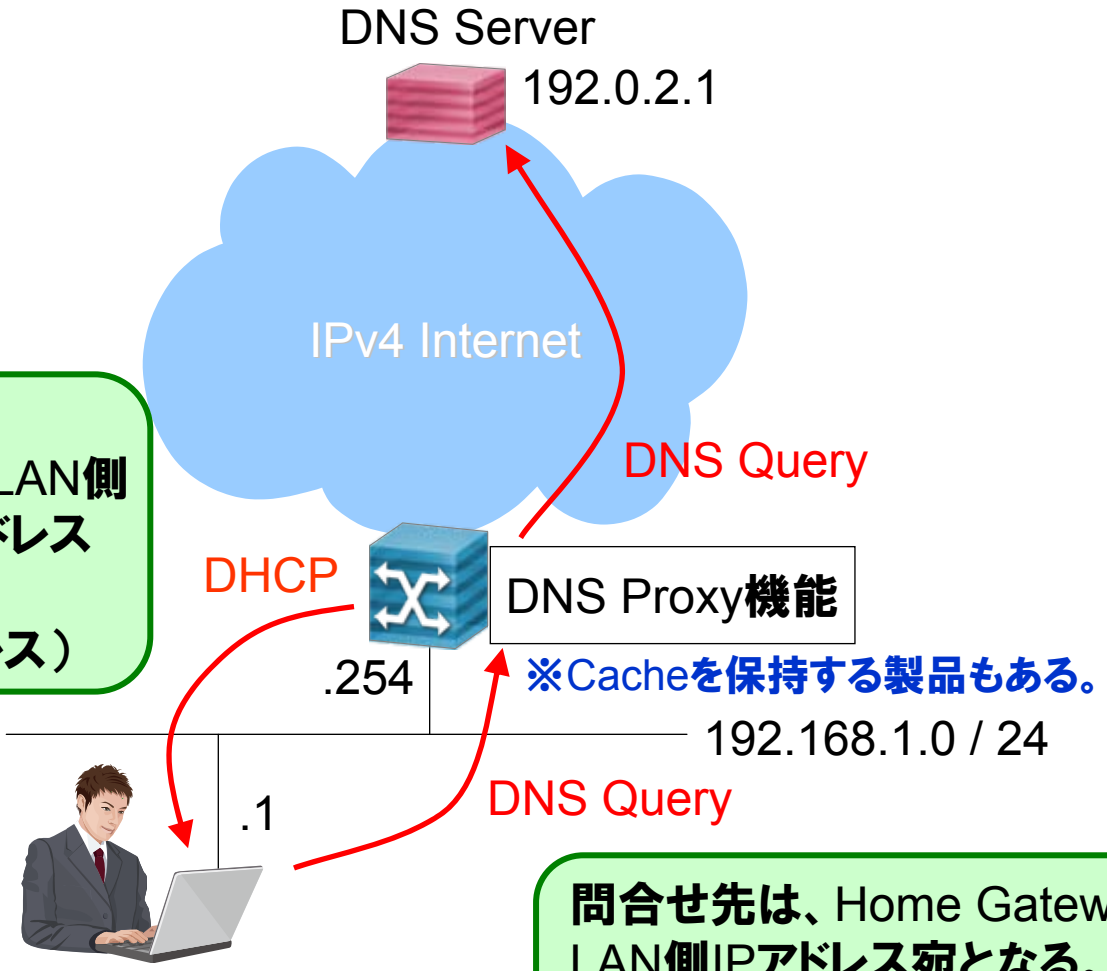
2010年 11月 25日

NECアクセステクニカ
アクセスネットワーク技術部
川島　正伸

目次

- Home Gateway の DNS Proxy 機能
- DNS Proxy 機能の必要性
- DNS Proxy の DNSSEC 対応
- DNS Cache は必要？
- DNS Proxy と IPv6
- その他の検討事項
- 参考情報
- オマケ

Home Gateway の DNS Proxy 機能



一般的には、
DHCPを使用してルータのLAN側IPアドレスをDNSサーバアドレスとしてホストに通知する。
（≠ISPのDNSサーバアドレス）

問合せ先は、Home Gateway のLAN側IPアドレス宛となる。
（端末からはHome Gatewayが DNS Server にみえる。）

DNS Proxy 機能の必要性

- Home Gateway の Web-GUI へのアクセスに使用
  - 装置設定を行う際に、web.setup 等の独自の FQDN を使用してアクセス可能となる。
    - IPアドレス直打ちよりも覚えやすく、一般ユーザには敷居が低い。
    - IPv6アドレスの場合、IPアドレス直打ちは困難。
- 複数の接続先が存在する場合の DNSサーバ選択問題の回避
  - インターネット接続とフレッツ閉域網接続など、管理ドメインが異なる複数の接続先がある場合、DNS Proxy 機能が適切なDNSサーバへ問合せを実施。
    - DNS Proxy 機能を提供しない場合、端末側で適切なDNSサーバを選択できない問題がある。
- DNS Cache を保持している場合、ISP の DNSサーバ負荷軽減や名前解決のレスポンスタイム短縮などのメリットあり。
  - 本当にメリット？デメリットは？（後ほど説明）

DNS Proxy の DNSSEC 対応（1）

- EDNS0（RFC2671）に対応
- Fragmented Packet を Reassemble
- TCP Transport にも対応
- 各種 Flags も透過的に扱う

DNS Proxy Implementation Guideline（RFC5625）に準拠した実装を行うとよい。

- 自社製ブロードバンドルータ（法人向け、民需向け）の動作検証を実施
  - JPRS の DNSSEC 技術実験に参加して検証
  - DNSSEC Hardware Tester（nic.cz が提供）を使用して検証

DNS Proxy の DNSSEC 対応（2）

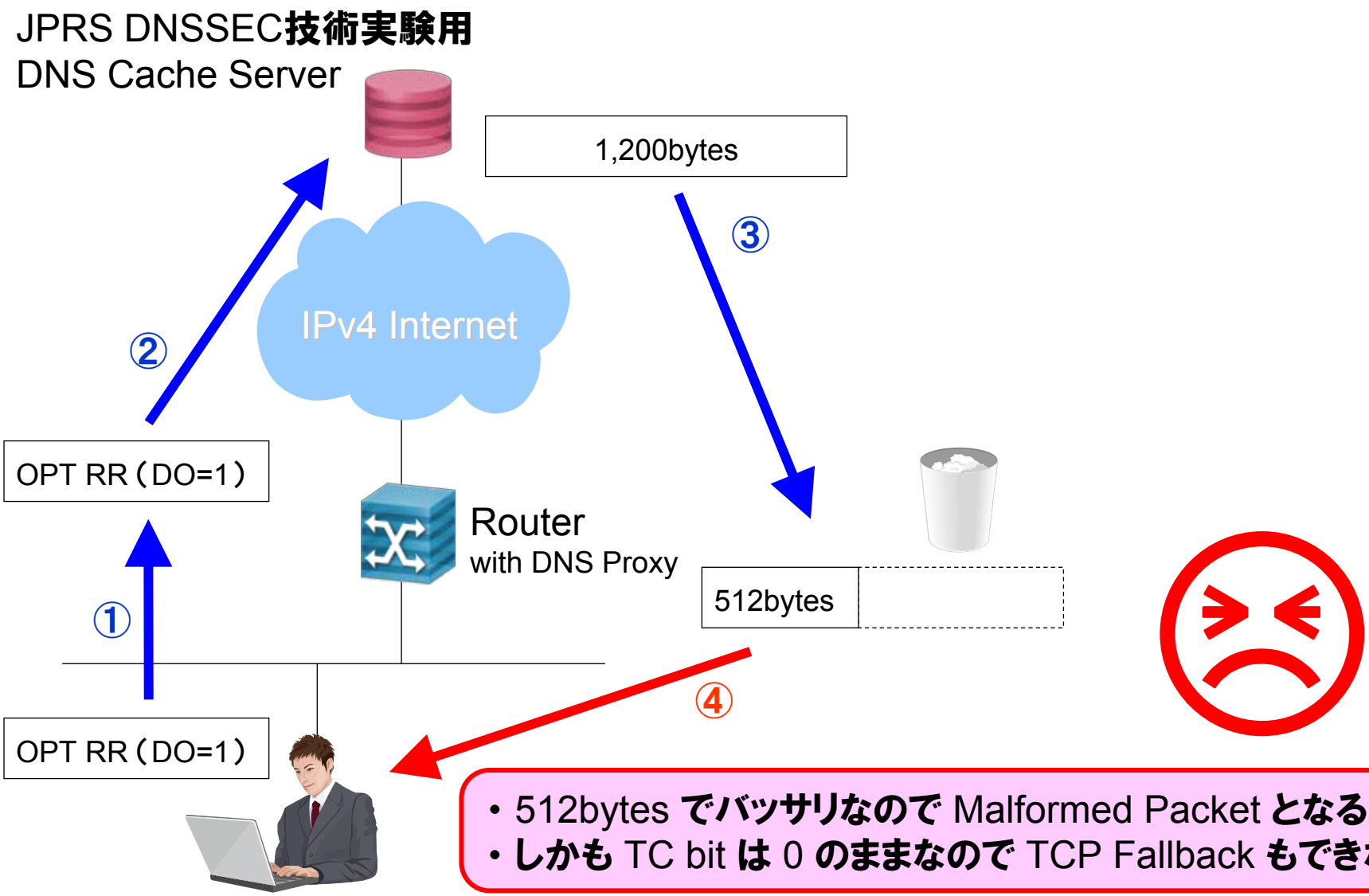
動作検証のポイント

- OPT RR（DO bit）や 各種 Flags（TC, AD, etc）を透過的に扱っているか？
- EDNS0 に対応し、1,220 bytes（MSG-SIZE）の Packet を処理できるか？　※Fragment なし
- EDNS0 に対応し、4,000 bytes（MSG-SIZE）の Packet を処理できるか？　※Fragment あり
- TCP Transport を使用した DNS Proxy を提供しているか？
- DNS Cache を行っている場合、悪影響はないか？

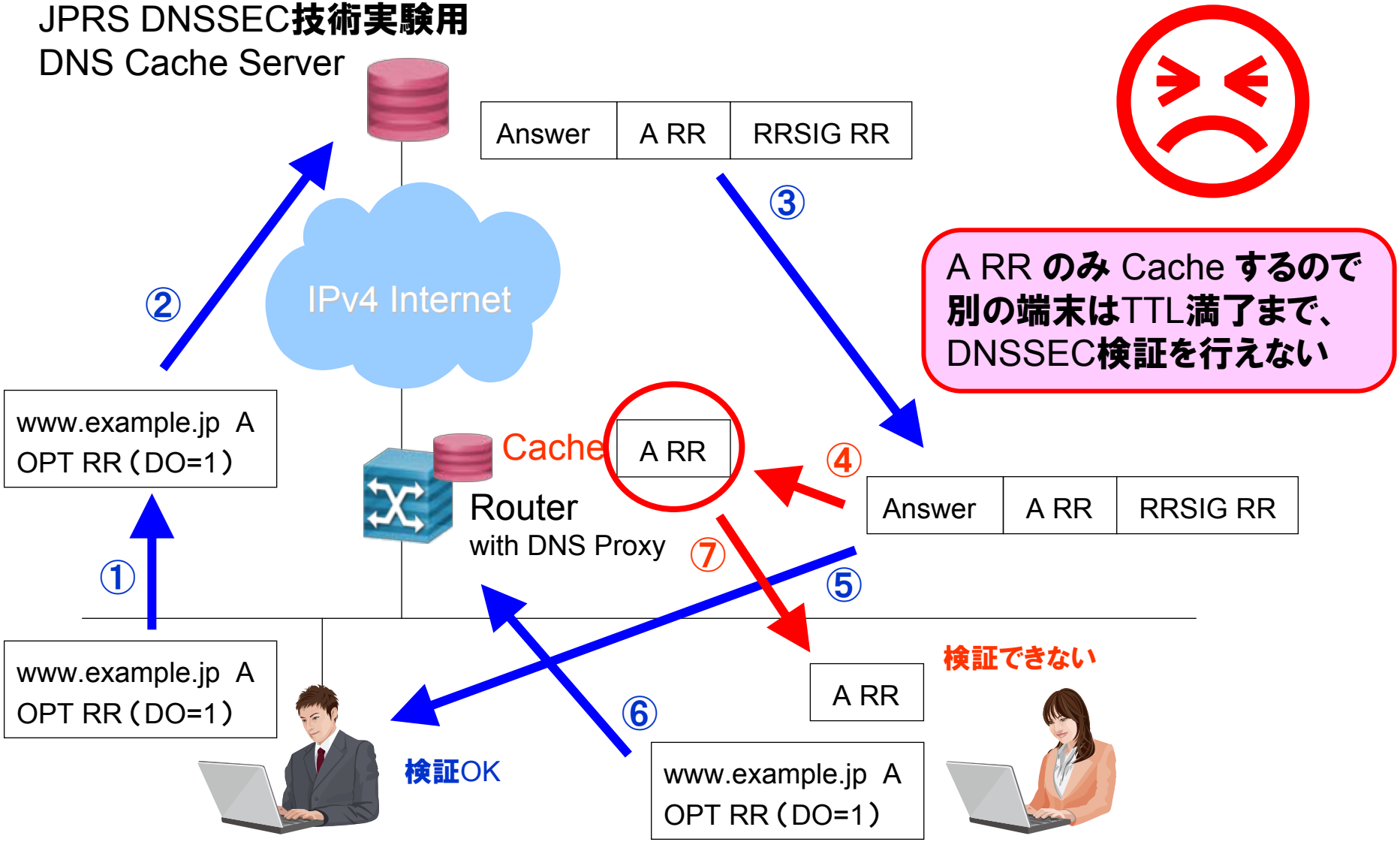
DNSSEC を考慮していない実装がありました。

もちろん良い実装も確認できました。

DNSSEC を考慮していない実装（DNS 512bytes の壁）

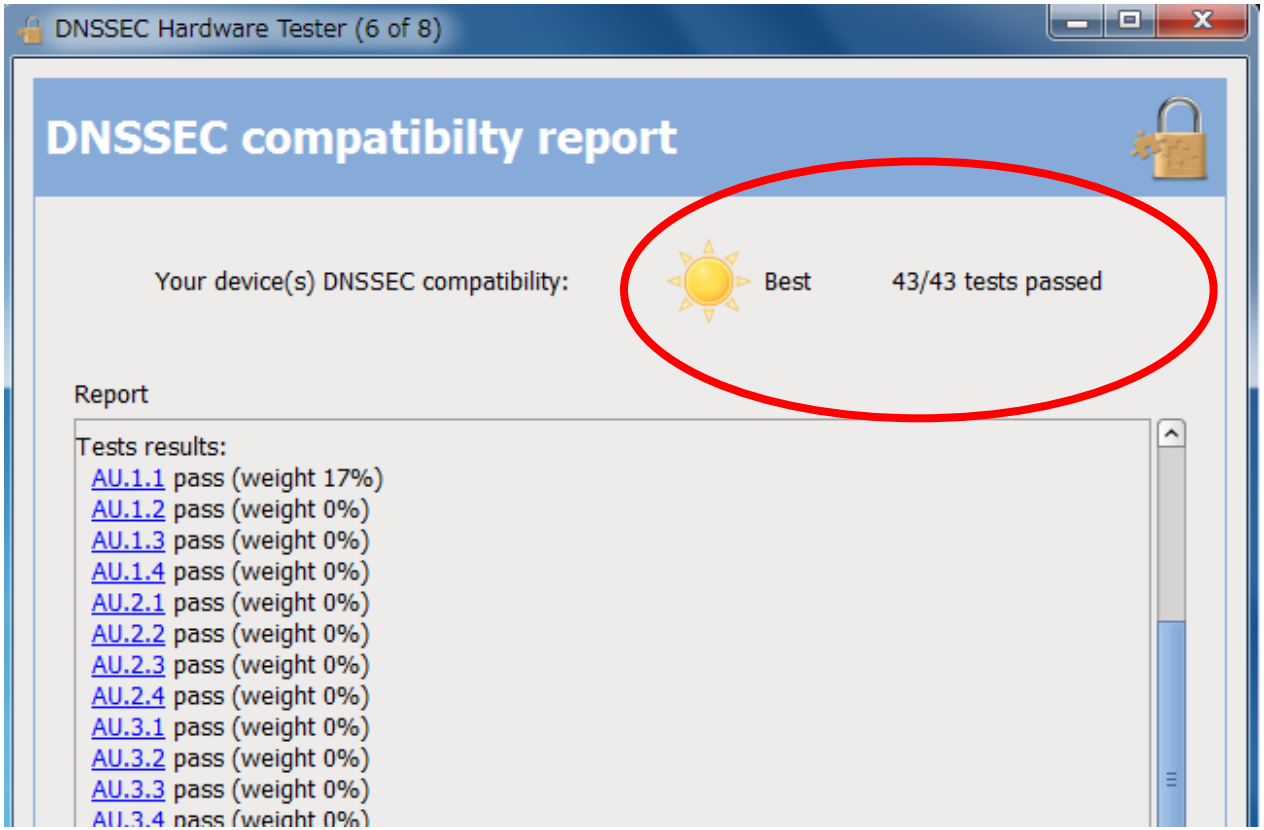


DNSSEC を考慮していない実装（Cache 不完全）



良い実装の話（1）

- nic.cz（**チェコの** TLD **レジストリ**）**が提供している** DNSSEC Hardware Tester **を使って** DNSSEC **の適合性チェックを実施してみました。**
  [合計43のテスト項目]



Best

43/43 tests passed

全項目パス！

良い実装の話（2）

- UNIVERGE WA1020（**法人向けモバイルルータ**）が DNSSEC 100% **適合一番乗り！**

（2010年7月8日時点）

TOP 10 DEVICES

	Device	Reports	Compatibility
1	NEC WA1020	8	100%
2	D-Link DGL-4300	1	92%
3	Edimax AR-7084gB	1	92%
4	Linksys WRT300N	1	92%
5	SMC SMCA1T-A	1	92%
6	TP-Link TD-W8910G	1	92%

No.1 Get !

2010/07/08 00:55 From NIC.CZ

“NEC WA1020” is the first appliance to achieve 100 % - even none of tested appliances in our lab so far was able to do so with default settings.

良い実装の話（3）

- 10月に発売した Aterm WR8370N シリーズ（コンシューマ向け高速無線LANルータ）も DNSSEC に対応しました。

（2010年11月11日時点）

TOP 10 DEVICES

	Device	Reports	Compatibility
1	NEC WA1020	8	100%
2	D-Link DIR-110	2	100%
3	NEC WR8370N	2	100%
4	D-Link DIR-815	1	100%
5	Netgear WNR3500L	1	100%
6	ZyXEL P-660R-63	2	95%
7	D-Link DGL-4300	1	92%
8	Edimax AR-7084gB	1	92%
9	Linksys WRT300N	1	92%
10	SMC SMCA1T-A	1	92%

Atermシリーズ新機種について、
今後も対応を予定しています。

DNS Cache は必要？（1）

メリット？

- ISP の DNSサーバ負荷軽減
  - 最近は、OS やブラウザ等でも Cache しているので、ルータでわざわざ Cache しなくても困らないのでは？
- 名前解決のレスポンスタイム短縮
  - Webアクセス等、トランザクションに占める DNS の割合は小さいし、回線のブロードバンド化の影響もあるので、名前解決のレスポンスタイムは無視できる範囲では？

デメリット

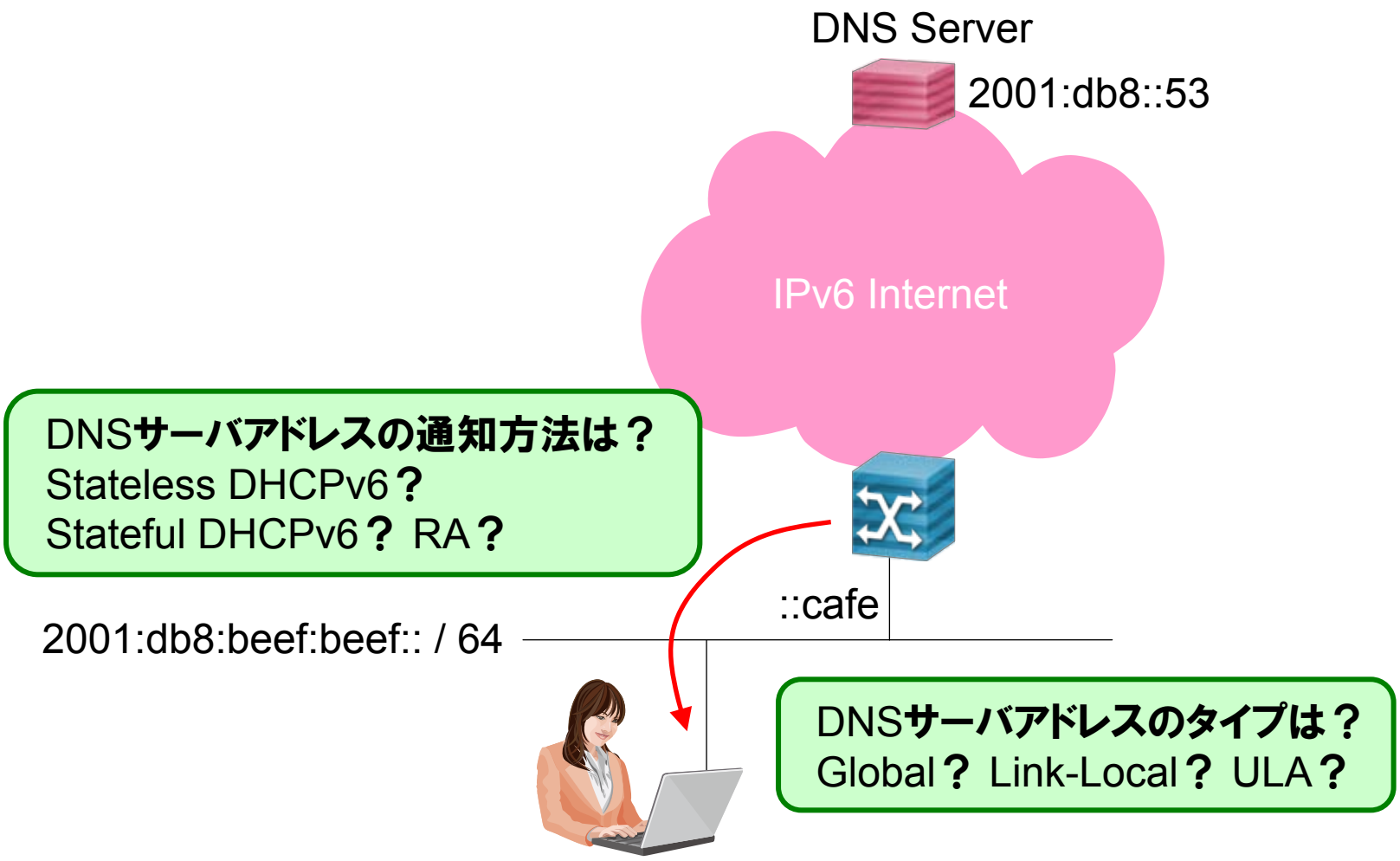
- Kaminsky Attack等の脆弱性対応に関して、迅速な対応が求められる。
  - ファームウェア修正後のバージョンアップ実施方法にも課題あり
- DNSSEC対応によるインパクト
  - 不完全な Cache 実装による問題への対処
  - RR SIG を Cache することによるリソース消費は懸念事項
  - Validator になるなら、署名検証処理の負荷は懸念事項

DNS Cache は必要？（2）

- どうやら、メリットよりもデメリットの方が多そう
- 実際のところ、どの程度効果があるか一般家庭を調査
  - 調査期間 ： 2010年4月14日～21日の 7日間
  - 家族構成 ： 父、母、娘、息子
  - スタブリゾルバ ： パソコン、ネット対応テレビ、ゲーム機、スマートフォン、等

- 調査結果
  - Total Query Count ： 20,731
  - Cache Hit Count ： 3,258
  - Cache Hit Rate ： 15.7％
  - リゾルバキャッシュを保持しない Node 数にキャッシュヒット率は比例
- 現時点での見解
  - DNS Proxy Implementation Guideline（RFC5625）的には、Transparent が大原則なので、不完全な Cache 実装を増やすよりも Cache しない方が望ましい。
  - ISP の DNSサーバへの負荷増の懸念については継続検討が必要。

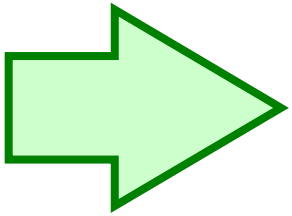
DNS Proxy と IPv6（1）



DNS Proxy と IPv6（2）

IPv4 と比較してみると。。。

	IPv4	IPv6
DNSサーバアドレスの通知方法	DHCPv4	Stateful DHCPv6 Stateless DHCPv6 RA Option
DNSサーバアドレス（待ち受けアドレス）	LAN側 IP Address	Link Local ULA Global Address



IPv4 はシンプル、 IPv6 は複雑に。

DNSサーバアドレスの通知方法

- IPv6 Router Advertisement for DNS Configuration（RFC5006）の Standards Track 化により、より複雑に。

RA Option	draft-ietf-6man-dns-options-bis が RFC Editor Queue に入っており、まもなく RFC化。 Experimental から Standards Track に変更。 DNS Search List も通知可能に。
Prefix情報 recursive DNS server DNS search list	

Stateless DHCPv6	RA Option の Standards Track 化により、 使途がやや不明確になってしまった。
---- 各種Option情報	

Stateful DHCPv6	RA（M-Flag ON, Default Route）に依存するが、 その他は自己完結可能。 自由度は高いので目的に応じて使用可能。
IP or Prefix情報 各種Option情報	

DNSサーバアドレス（DNS Proxy の待ち受けアドレス）

Link Local Address

- ネットワークを越えた通信はできないので、配下に別のルータが存在している環境（他セグメントとの通信）では使用できない。
- Link Local Address が指定できないホストも存在するらしい。

Unique Local Address

- Global ID生成、DAD処理などが必要。Prefix通知はケースバイケース。
- Global ID生成を RFC に従うべきか、あるいはわかりやすい固定値とするかは悩みどころ。

Global Address

- WAN Link Down 時やセットアップ未完了時などにアドレスを通知できない。また、端末との情報の不整合が発生する可能性あり。

いずれのアドレスも一長一短があり、使用環境に応じた使い分けが必要である。

その他の検討事項

- DNSSEC における Last 1 Hop（DNS Server ー Host 間）は、どのようにしてセキュリティを担保するのか？
  - Windows 7 では、IPsec を使用することを想定しているようだが、その場合、Home Gateway が IPsec を終端すべきか否か。

- Home Gateway 自身のリゾルバは、いつから DNSSEC 対応を考慮すべきか？
  - Ping や Traceroute 以外に、Home Gateway 自身が名前解決を行うことも多い。

- その他にも、TCPフォールバック問題、DNSサーバ選択、トランスポート／リソースレコード変換、Dynamic DNS、等々 Home Gateway や DNS周辺の検討事項は多い。

参考情報（1）

IETF

- RFC5625 DNS Proxy Implementation Guideline
- RFC4035 Protocol Modifications for the DNS Security Extensions
- RFC2671 Extension Mechanisms for DNS（EDNS0）
- draft-ietf-dnsext-rfc2671bis-edns0（work in progress）
- RFC5966 DNS Transport over TCP - Implementation Requirements
- RFC4472 Operational Considerations and Issues with IPv6 DNS
- draft-ietf-v6ops-ipv6-cpe-router Basic Requirements for IPv6 Customer Edge Routers（work in progress）
- RFC5006 IPv6 Router Advertisement Option for DNS Configuration
- draft-ietf-6man-dns-options-bis IPv6 Router Advertisement Options for DNS Configuration（work in progress）
- HOMENET WG home networking working group（Proposed Working group）

参考情報（2）

Broadband Forum

- TR-124 Issue-2 Functional Requirements for Broadband Residential Gateway Devices

IPv6普及・高度化推進協議会

- IPv6家庭用ルータガイドライン 2.0版

DNSSEC 動作検証

- JPRS DNSSEC技術実験への参加
- DNSSEC Hardware Tester（http://www.nic.cz/dnssectests/）

［オマケ］IPv6アドレスの推奨テキスト表記

IPv6アドレス表記が統一されていない問題を解決したい。

- ［RFC5952］A Recommendation for IPv6 AddressText Representation **として、標準化されました！**
  http://www.rfc-editor.org/rfc/rfc5952.txt

従来表記

2001:0db8:0000:0000:abcd:0000:0000:0001
2001:db8:0:0:abcd:0:0:1
2001:db8:0:0:abcd::1
2001:DB8::ABCD:0:0:1
etc

推奨表記

2001:db8::abcd:0:0:1

皆さまがお使いのシステムや製品にて、RFC5952 への準拠をお願い致します。

Empowered by Innovation