

動かしてみました DNSSEC

ー ブロードバンドルータ編 ー

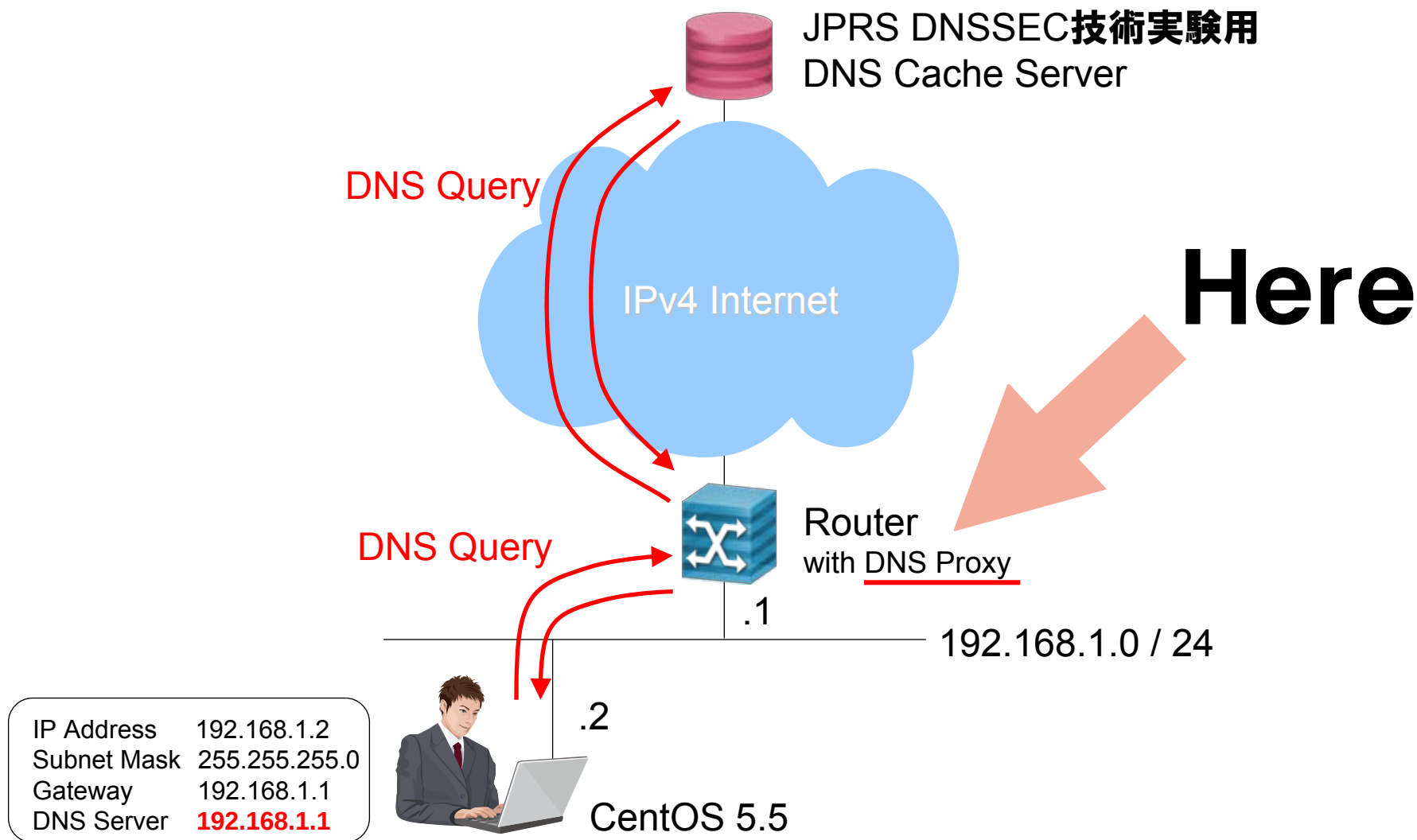
2010年 7月 8日

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

JPRSさんのDNSSEC技術実験に参加して
自社製ブロードバンドルータ(法人向け、民需向け)
の DNS Proxy 機能を動作検証してみました。



検証構成



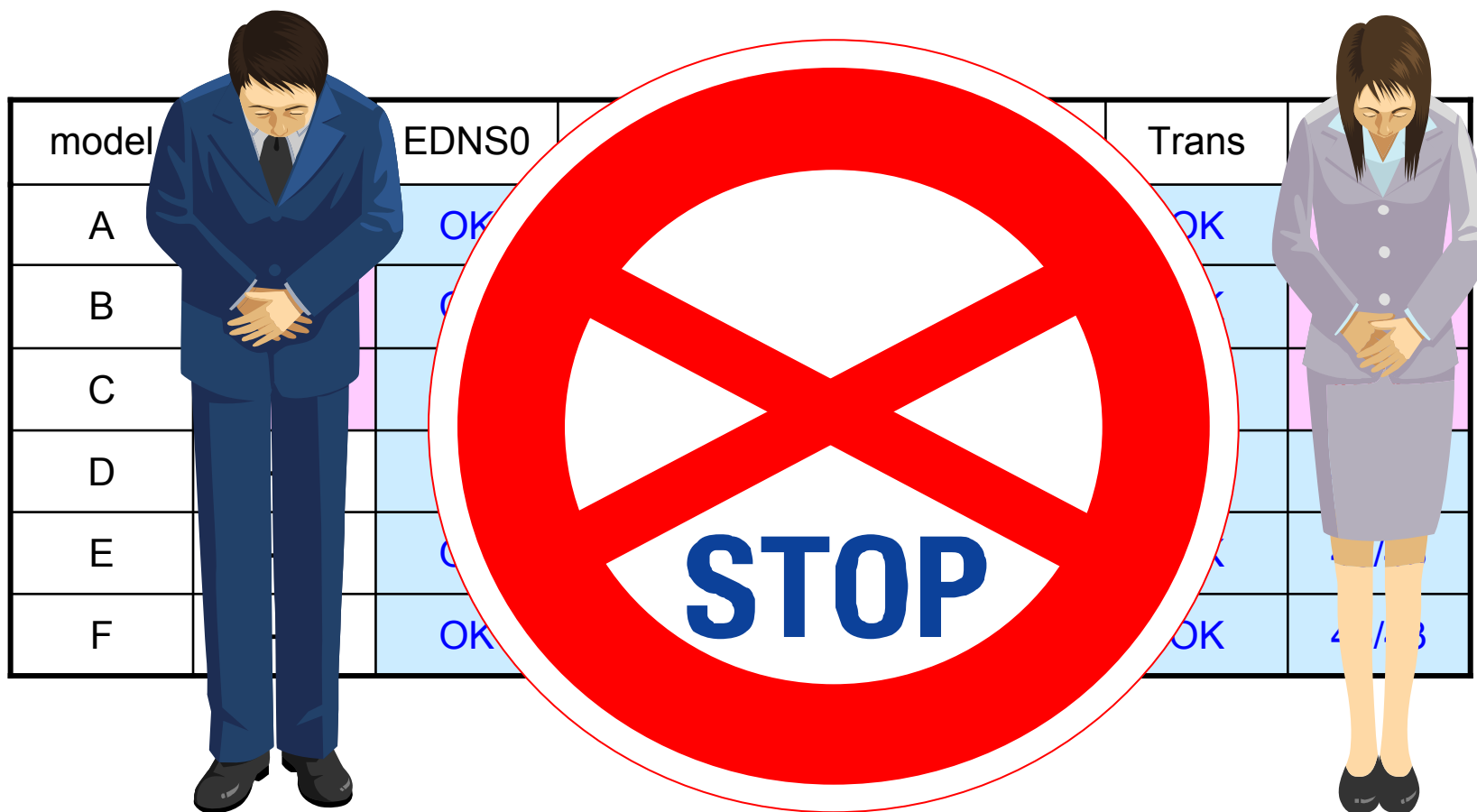
検証のポイント

- 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 の Packet を処理できるか？
※Fragment されていない
- EDNS0 に対応し、4,000 bytes の Packet を処理できるか？
※Fragment されている
- TCP を使用した DNS Proxy 機能を提供しているか？
- DNS Cache を行っている場合、何か悪影響はないか？

検証結果

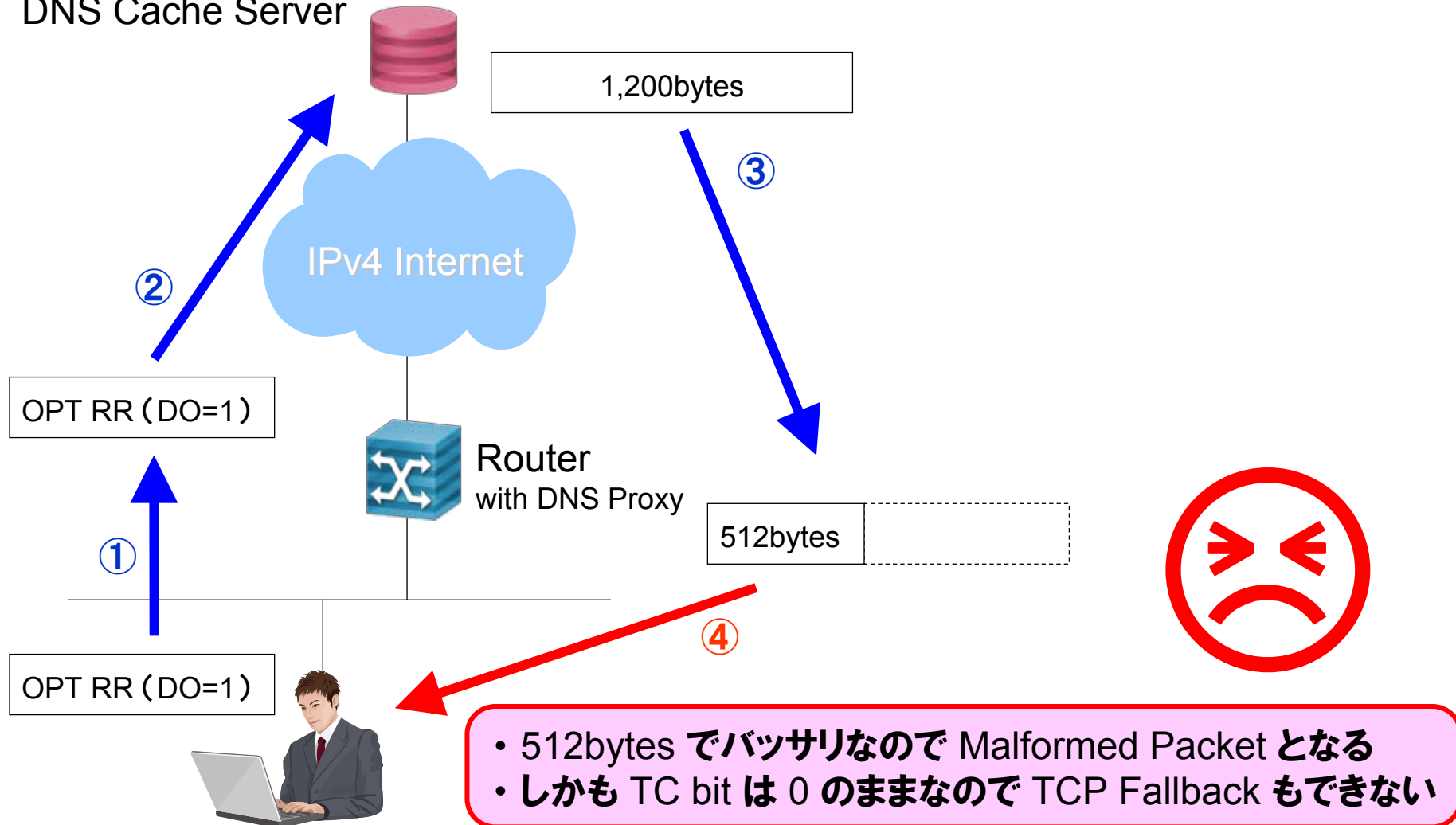
イケてる実装とイケてない実装がありました

- でも具体的な説明はできません。ごめんなさい。。



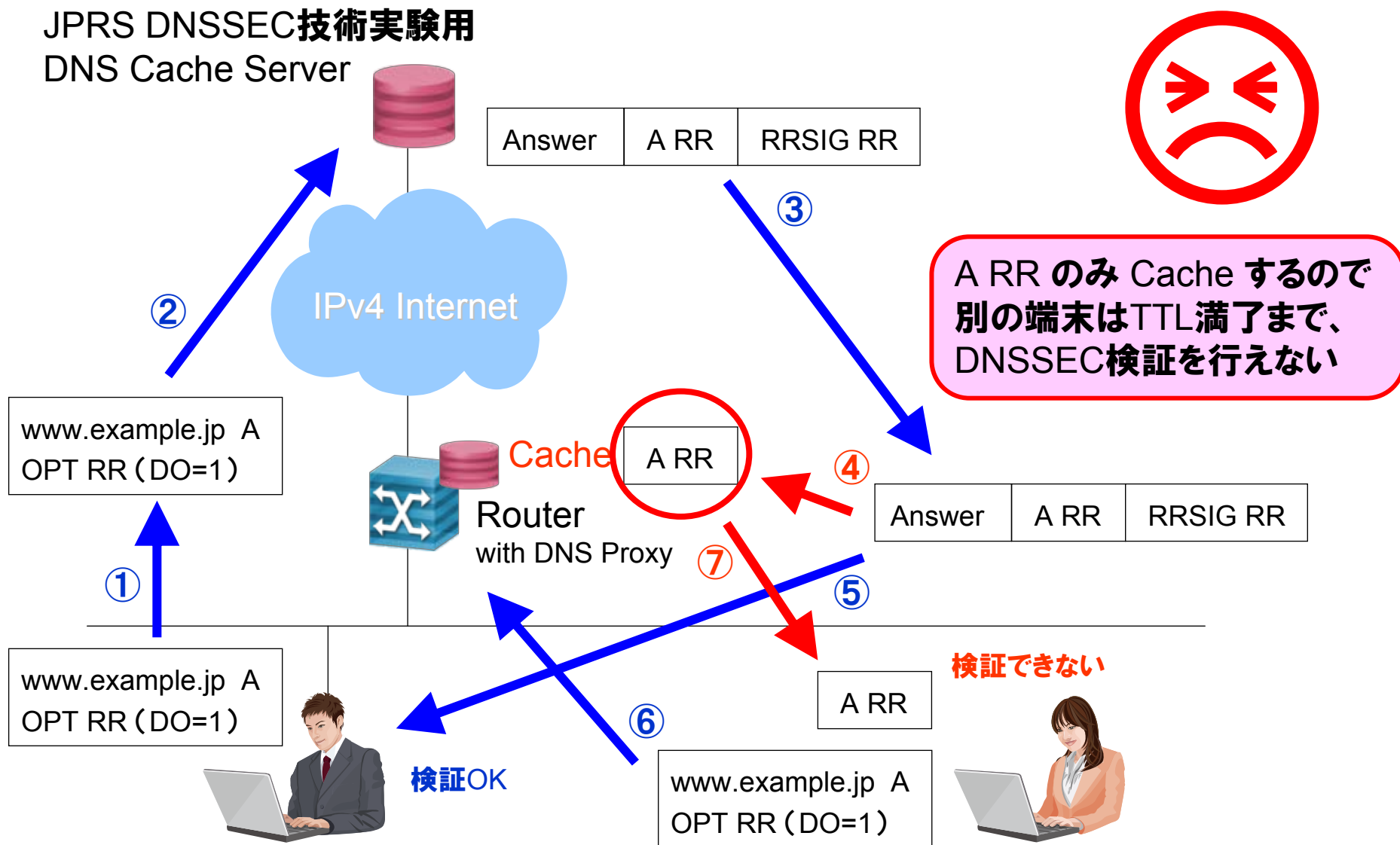
イケてない実装の話 その1 (512bytesへの異常な愛)

JPRS DNSSEC技術実験用
DNS Cache Server



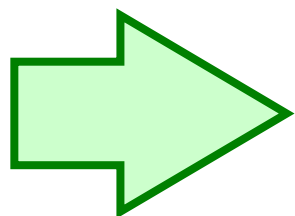
イケてない実装の話 その2 (なんちゃってキャッシュ)

JPRS DNSSEC技術実験用
DNS Cache Server



イケてる実装の話

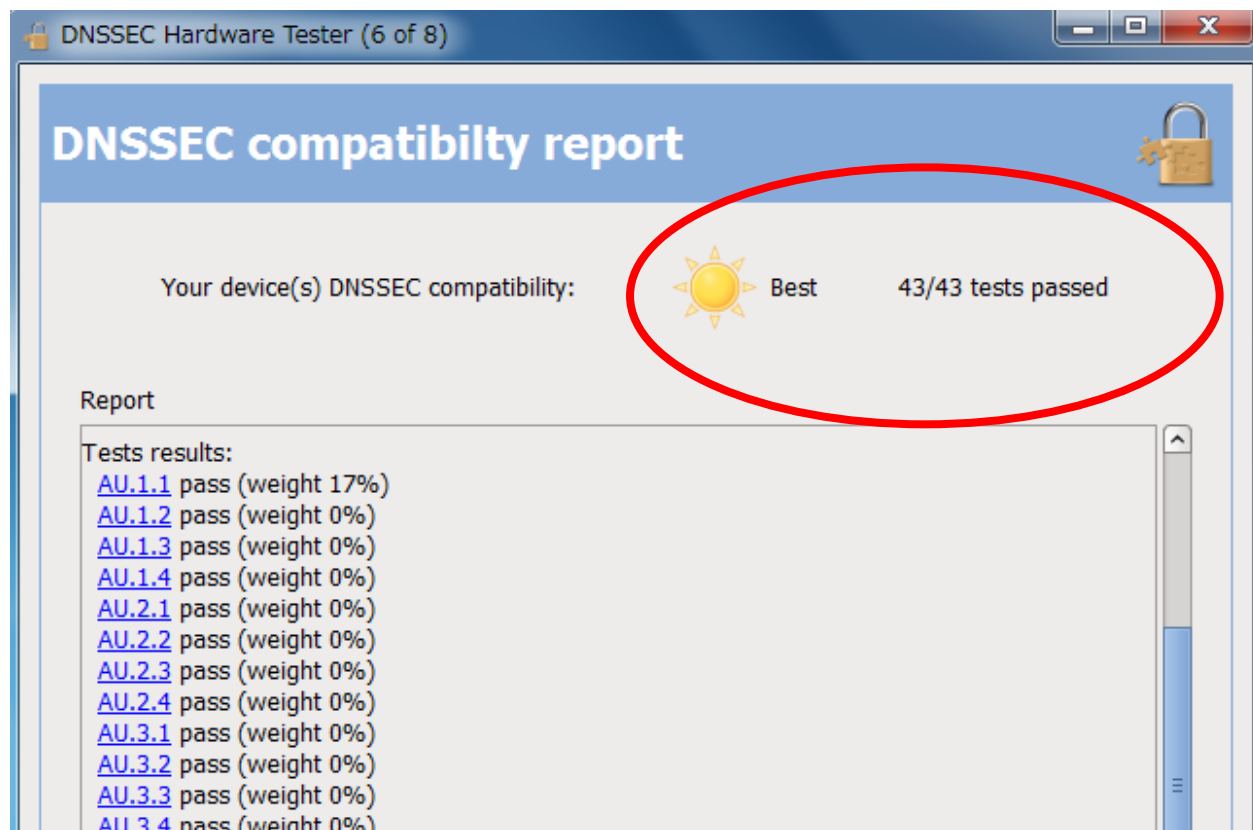
- EDNS0 に対応
- Fragmented Packet を Reassemble
- TCP にも対応
- 各種 Flags も透過的に扱う



RFC5625 DNS Proxy Implementation Guideline
に準拠した実装

イケてる実装の話（続き）

ついでに nic.cz (チェコのTLDレジストリ) が提供しているツール (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！



イケてる実装の話（続き）

そして、もちろんテスト結果を報告。



MOST TESTED		TOP 10 DEVICES		
Manufacturer	Reports	Device	Reports	Compatibility
1 Cisco	15	1 NEC WA1020	8	☀️ 100%
2 AVM FRITZ	12	2 D-Link DGL-4300	1	☀️ 92%
3 Linksys	11	3 Edimax AR-7084gB	1	☀️ 92%
4 D-Link	9	4 Linksys WRT300N	1	☀️ 92%
5 NEC	8	5 SMC SMCA1T-A	1	☀️ 92%



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.

No.1 Get !



今後の対応

**修正が必要な実装については、
良い実装をベースに計画的に展開していく予定です。
(でも、古い機種とかはごめんなさい。。。)**



まとめ

OPT RR (DO bit) や 各種 Flags (TC, AD, etc)を透過的に扱う実装とすること

- 不要なトラブルを引き寄せないためにも

EDNS0 に対応し、UDP 4,096bytes 迄をサポートすること

- Fragmented Packet を Reassemble すること

TCP に対応し、65,535bytes 迄をサポートすること

- 多くの DNS Proxy は TCP に対応していない

DNSSEC対応に限らず、応答Packet Size は肥大化傾向

- いずれにせよ EDNS0対応、TCP対応は必要

DNS Cache は行わないのが得策

- Cache する場合、考慮事項は多いので覚悟して実装すること

■ DNS Proxy 開発時の参考ドキュメント

- RFC5625
DNS Proxy Implementation Guideline
- RFC4035
Protocol Modifications for the DNS Security Extensions
- draft-ietf-dnsext-dns-tcp-requirements-03 (work in progress)
DNS Transport over TCP - Implementation Requirements
- 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
Coming Soon !

■ DNSSEC 動作検証

- JPRS DNSSEC技術実験への参加
- DNSSEC Hardware Tester (<http://www.nic.cz/dnssectests/>)
 - 現状、Windows 7 では Bug (結果報告できない) があるので注意。
テスト自体は問題ありません。



Empowered by Innovation

NEC