DNSSEC 技術実験報告書

機能・性能確認編

株式会社日本レジストリサービス
http://日本レジストリサービス.jp/
http://jprs.co.jp/
2010-09-06 Ver. 1.0

目次

DNSSEC技術実験概要

DNSSEC を導入すると、DNS データには電子署名(以下、署名)が付加される。DNS データを利用する側では署名を検証する必要があり、計算コストが増加する。また署名が付加されるため、従来の DNS では 512 バイトの制限があった DNS パケットが EDNS0 との組合せにより大きな DNS パケットとなる。この大きさは条件によっては一般的な MTU サイズである 1500 バイトを超える程大きくなる場合もあり、IP フラグメントを考慮する必要がある。

このような DNS パケットサイズの増大は、そのまま DNS トラフィックの増加につながり、DNS のキャッシュにも影響を与えることになる。また DNS パケットが通信するネットワーク機器なども影響が予想される。

JP ゾーンに DNSSEC を導入した際、JP のみならずルート DNS サーバやキャッシュ DNS サーバなどの連携する DNS サーバ群全体やネットワーク接続機器などに影響が生じることが予想される。その影響を事前に確認しスムーズなサービス導入に結びつけるため、実験環境を構築して実験を行った。

この実験を通じて、キャッシュ DNS サーバ、権威 DNS サーバ、ネットワーク接続機器等に DNSSEC を導入した場合の影響に関する知見を得ることができた。

実験に先立ち JPRS では、各 DNS サーバにおいて正しく DNSSEC サービスを提供できるようにするために必要な各種動作を確認するため、次の 2 種類の手順書を用意した。

「DNSSEC 機能確認手順書」
「DNSSEC 性能確認手順書」

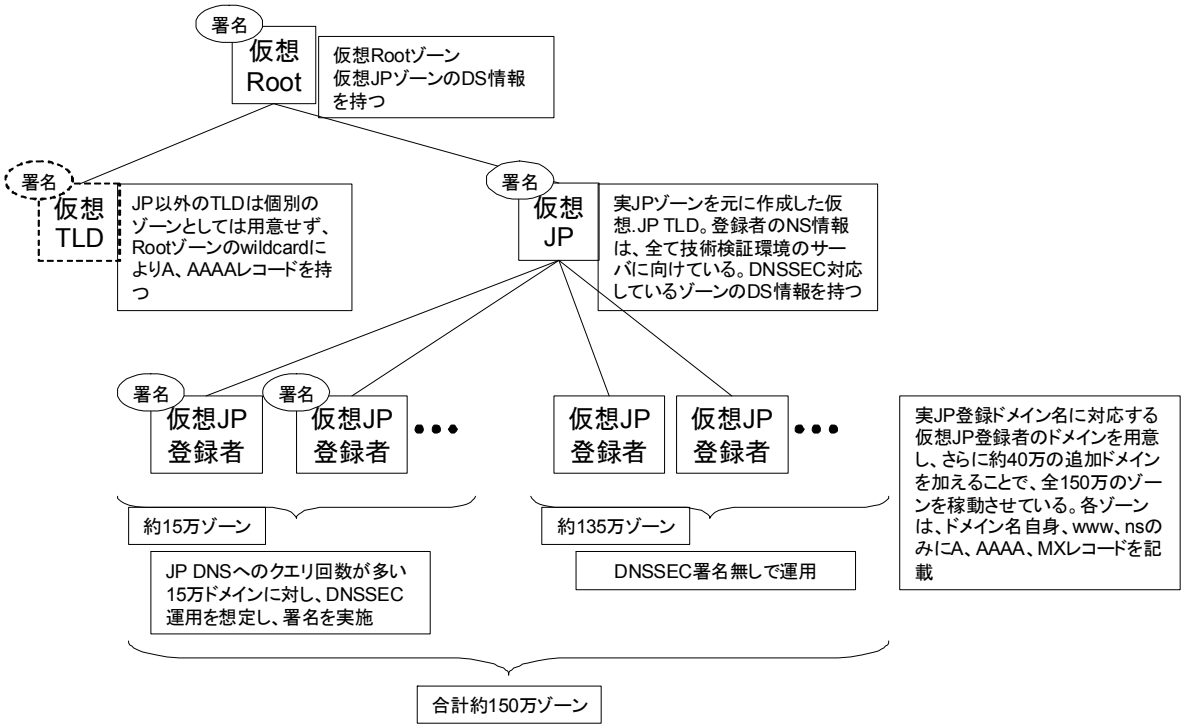
技術実験の一部では本手順書に記載されている確認手順に従って実験を行っているため、これらもあわせて参照されたい。手順書は以下の URL より入手できる。

DNSSEC 関連情報 <http://jprs.jp/dnssec/>

DNSSEC技術実験環境

仮想DNSツリー

DNSSEC 技術実験を行うための環境として、JPRS では実在する JP ドメイン名を基に以下の図に示すような仮想 DNS ツリーを構築した。



上図には含まれていないが、比較対象として JP ゾーンの署名対象ドメイン名を未署名(通常の DNS のツリーと同じ)とした仮想ツリーも構築し、DNSSEC の有無による比較が行える環境を用意した。また仮想 DNS ツリーを参照するキャッシュ DNS サーバも用意した。

実験方法

実験参加者がキャッシュ DNS サーバの試験を行う場合、インターネットに接続した仮想ツリーを参照する実験用キャッシュ DNS サーバを配し、負荷生成装置などを使用して DNS クエリを発生させ、キャッシュ DNS サーバの負荷(応答性能、CPU 占有率、メモリ使用量、in/out パケットサイズ等)を計測し、DNSSEC 対応した場合の変化を測定した。

またハードウェア機器の試験では、実験参加者がインターネットに接続した確認対象となる実

験用機器を配し、当該機器を通して DNS クエリを送受信し、DNSSEC 対応のパケットが正常に送受信されるかを確認した。

機能確認結果

機能確認 事例 1

■ 事例 1 実験環境

■ 事例 1 実験結果概要

機能面はほぼシナリオ通り機能確認を実施。

問題は特になし。

■ 事例 1 実験結果詳細

IPv6 での試験は、環境が準備できず機能評価は実施できていないが、

それ以外は概ねシナリオ通り評価を実施。特に問題点はない。

■ 事例 1 得られた知見

・ NSEC3 使用、鍵長 1024bit の ZSK で署名すると、ZSK 一つでゾーンファイルの容量は

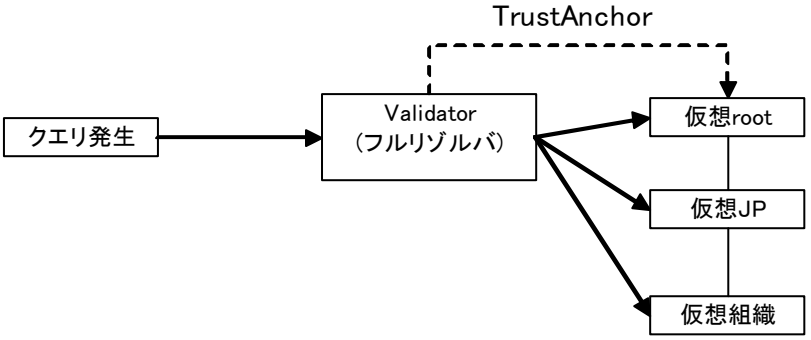
約 10 倍になる。

・ 実際の運用の場では DNSSEC 周りの問題の切り分けマニュアルの整備が必要。

機能確認 事例 2

■ 事例 2 実験環境

サーバ構成	使用アプリケーション
仮想 root 仮想 JP 仮想組織 validator クエリ発生	BIND9.7.1-P2 queryperf 改造版 resperf



■ 事例 2 実験結果概要

署名無→署名有になるとリソースが以下のように変化する

CPU 使用率　　約 2 倍

メモリ使用量　　約 3 倍

NW 帯域(query)　　約 2 倍

NW 帯域(Reply)　　約 4 倍

■ 事例 2 得られた知見

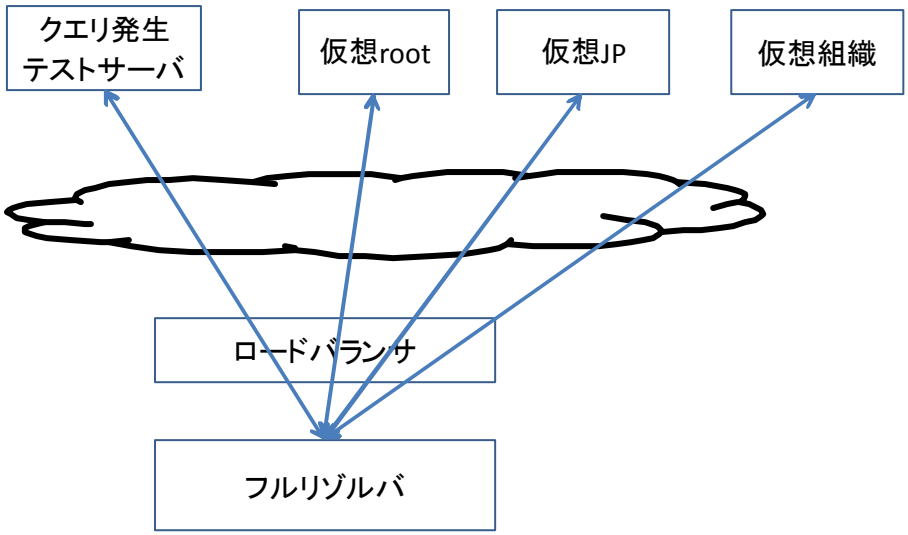
キャッシュに蓄積されるデータサイズが肥大化する

CPU 使用率、メモリの肥大化だけではなく、鍵の保存、ZONE の署名等によって HDD リソースも増大する

パケット数及びデータサイズの肥大化によって NW 帯域も圧迫される

機能確認 事例 3

■ 事例 3 実験環境



機能	HW	アプリケーション	備考
フルリゾルバ	SUN X2100 Solaris10	bind-9.7.0	IPv4 のみ
ロードバランサ	A10networks AX2500		IPv4 のみ
クエリ発生	SUN NetraT1	queryperf 改造版	IPv4 のみ

■ 事例 3 実験結果概要

JPRS 提供の DNSSEC 機能確認手順書 Ver. 1.1 の Ⅳ. 確認項目におけるフルリゾルバ側及び、共通項目のうち、以下項目について問題なく実施しできたことを確認した。

2. フルリゾルバ側

確認項目 F-2. DNSSEC 対応フルリゾルバの利用による AD ビットの確認

確認項目 F-27. RRSIG レコードの有効期間終了フィールドが現在時刻より後であること

確認項目 F-28. RRSIG レコードの有効期間開始フィールドが現在時刻より前であること

確認項目 F-47. DS レコードのアルゴリズムは対応する DNSKEY レコードのものに一致するべき

確認項目 F-49. DS レコードのダイジェストは対応する DNSKEY レコードの鍵のハッシュであるべき

確認項目 F-85. セキュリティ対応フルリゾルバは EDNS0 による UDP 通信が可能である

確認項目 F-86. セキュリティ対応フルリゾルバは 1220 バイトの UDP メッセージをサポートしていること

確認項目 F-87. セキュリティ対応フルリゾルバは 4000 バイトの UDP メッセージをサポートすべき

確認項目 F-130. セキュリティ対応フルリゾルバは元の問い合わせの DO ビットに関わらず、再帰検索においては DO ビットを設定していること

確認項目 F-147. セキュリティ対応フルリゾルバの IP 層は IPv4 か v6 かに関わらず、フラグメントされた UDP パケットを正しく処理できなければならない

⇒IPv4 のみ実施

確認項目 F-154. セキュリティ対応フルリゾルバは少なくとも 1 つの信頼できる公開鍵または DS を設定に組み込める機能を持たねばならない

確認項目 F-194. 自分自身で署名され REVOKE bit の立った DNSKEY は Revoke される

確認項目 F-196. Revoke された DNSKEY は trust anchor として使用されない

確認項目 F-201. タイマー期限が過ぎたら新しい鍵は trust anchor に追加されること

確認項目 F-202. タイマー期限が来る前に新しい鍵は trust anchor に追加されていないこと

確認項目 F-229. ゾーンの頂点に NSEC3PARAM レコードが存在すること。

3. 共通項目

確認項目 共通-1. TCP の通信がブロックされていないことの確認

確認項目 共通-2. BIND の設定において、署名したゾーンファイルが BIND に読み込まれていることの確認

確認項目 共通-3. BIND の設定ファイルにおいて DNSSEC が有効になっていることの確認

確認項目 共通-4. ping コマンドによる通信経路の MTU の確認

■ 事例 3 実験結果詳細

特記事項なし

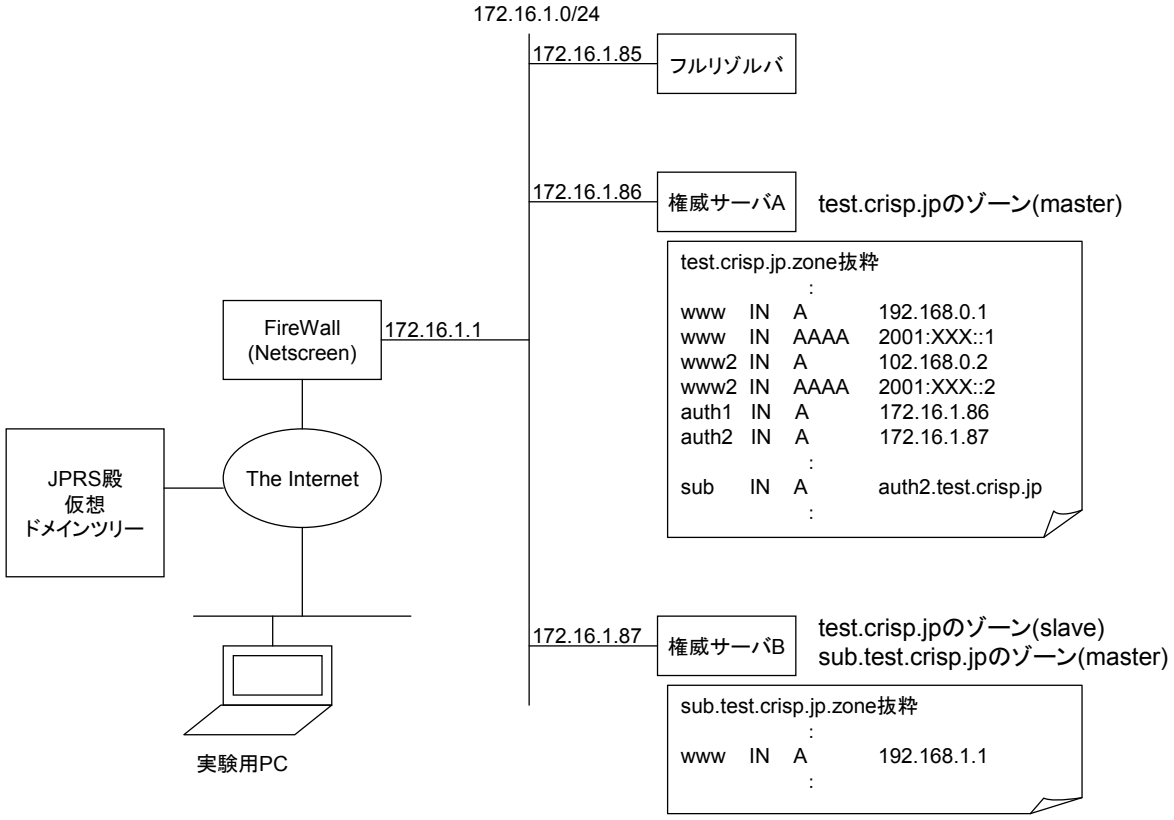
■ 事例 3 得られた知見

上記環境にて、各項目に基づいたテストを実施しましたが、特に不具合はありませんでした。よって、DNSSEC 導入における機能的な問題はないものと考えます。

機能確認 事例 4

■ 事例 4 実験環境

・実験環境構成



・ソフトウェア構成

OS：Solaris10　BIND：9.7.0-P1

■ 事例 4 実験結果概要

【DNSSEC 機能確認手順書 Ver.1.1】の確認手順に基づき、以下の試験を実施。
すべてのシナリオにおいて想定の挙動であることを確認するとともに、各シナリオのケースにおけるクライアントおよびサーバ側の状況を確認した。

【シナリオ 1】 権限サーバへの問い合わせに常に失敗する
【シナリオ 2】 権限サーバへの問い合わせに時々失敗する
【シナリオ 3】 権限サーバへの問い合わせが遅い
【シナリオ 4】 権限サーバへの問い合わせの結果が不正
【シナリオ 5】 フルリゾルバへの問い合わせが失敗する

【シナリオ 6】 フルリゾルバへの問い合わせが時々失敗
【シナリオ 7】 フルリゾルバへの問い合わせが遅い
【シナリオ 8】 フルリゾルバが問い合わせの検証に失敗
【シナリオ 9】 フルリゾルバが問い合わせの結果異常

■ 事例 4 実験結果詳細

シナリオ 1

①テスト機のネットワーク的な問題
実施 →問題なし

②テスト機-権限サーバ間の問題
実施 →問題なし

③512 オクテットを超えるパケットの問題
<A-85>実施 → 問題なし
<A-86>実施 → 問題なし

(補足)
各試験項目において、EDNS0 による UDP 通信、TCP への切替り、およびフラグメント通信を確認

シナリオ 2

①問い合わせの内容が同じでも、成功/失敗が発生する
実施 → 問題なし

②問い合わせの内容により、成功/失敗が変化する
シナリオ 1 の試験<A-85>にて充当

(補足)
各試験項目において、EDNS0 による UDP 通信、TCP への切替り、およびフラグメント通信を確認
NW 環境の制限により、問い合わせの成功/失敗が変化することを確認

シナリオ 3

①別の権威サーバに対しても、遅い
ネットワーク遅延環境の準備が間に合わず未実施

②別の権限サーバでは問題がない
シナリオ 1 試験<A-85>により充当
TCP/UDP/フラグメント等により通信内容が変化することを確認
(遅延が発生する可能性は確認できるも、NW 遅延環境は構築できず)

シナリオ 4
①DNSKEY レコード異常
<A-27>実施 → 問題なし
<A-28>実施 → 問題なし
<A-58>実施 → 問題なし
<A-61>実施 → KSK の署名なしでの signzone ができなかったため未実施
<A-79>実施 → 問題なし

②RRSIG レコード異常
<A-27,28>シナリオ 4-1 の試験結果にて充当
<A-76>実施 → 問題なし(A-79 と同時に実施)
<A-95>実施 → 問題なし
<A-115>実施 → 問題なし

④NSEC レコード異常
実施 → 問題なし

⑤DS レコード異常
<A-47>実施 → 問題なし
<A-76>シナリオ 4-2 にて実施
<A-78>実施 → 問題なし
<A-79>シナリオ 4-1 にて実施
<A-81>TTL に差異を作れなかったため未実施

⑥NSEC3PARAM レコード異常
NSEC3 を利用していなかったため未実施 → 別途実施

⑦NSEC3 レコード異常
NSEC3 を利用していなかったため未実施 → 別途実施

シナリオ 5
①テスト機のネットワーク的な問題

実施 → 問題なし

②テスト機 – フルリゾルバ間の NW 的な問題
実施 → 問題なし

③フルリゾルバ – 権威サーバ間の NW 的な問題
実施 → 問題なし

④フルリゾルバ – 権威サーバ間の問い合わせ
実施 → 問題なし

⑤フルリゾルバの設定の問題
<F-85>実施 → 問題なし
<F-86>実施 → 問題なし
<F-87>実施 → 問題なし
<F-130>実施 → 問題なし
<F-147>実施 → 問題なし(ただし v6 環境は未実施)

シナリオ 6
①問い合わせが同じでも 成功/失敗が発生する
シナリオ 5 試験により充当

②問い合わせの内容により 成功/失敗が発生する
<F-85>実施 → 問題なし

シナリオ 7
①フルリゾルバから権威サーバへの問い合わせが遅い
ネットワーク遅延環境の準備できず未実施
②テスト機-フルリゾルバ間の NW の問題
ネットワーク遅延環境の準備できず未実施

③フルリゾルバの設定の問題
シナリオ 5 試験により充当

シナリオ 8
①フルリゾルバの DNSSEC が無効
<F-130>実施 → 問題なし

②フルリゾルバのトラストアンカーに問題
<F-154>実施 → 問題なし
<F-201>未実施

③フルリゾルバの時刻設定の問題
シナリオ 8-5 試験にて充当

④DS レコードと DNSKEY レコードの連鎖の問題
<A-47>実施 → 問題なし
<A-76>実施 → 問題なし
<A-78>実施 → 問題なし
<A-79>実施 → 問題なし
<A-81>実施 → 問題なし
<A-115>実施 → 問題なし

⑤DNSSEC の署名に問題
<A-27>実施 → 問題なし
<A-28>実施 → 問題なし
<A-58>実施 → 問題なし
<A-115>実施 → 問題なし

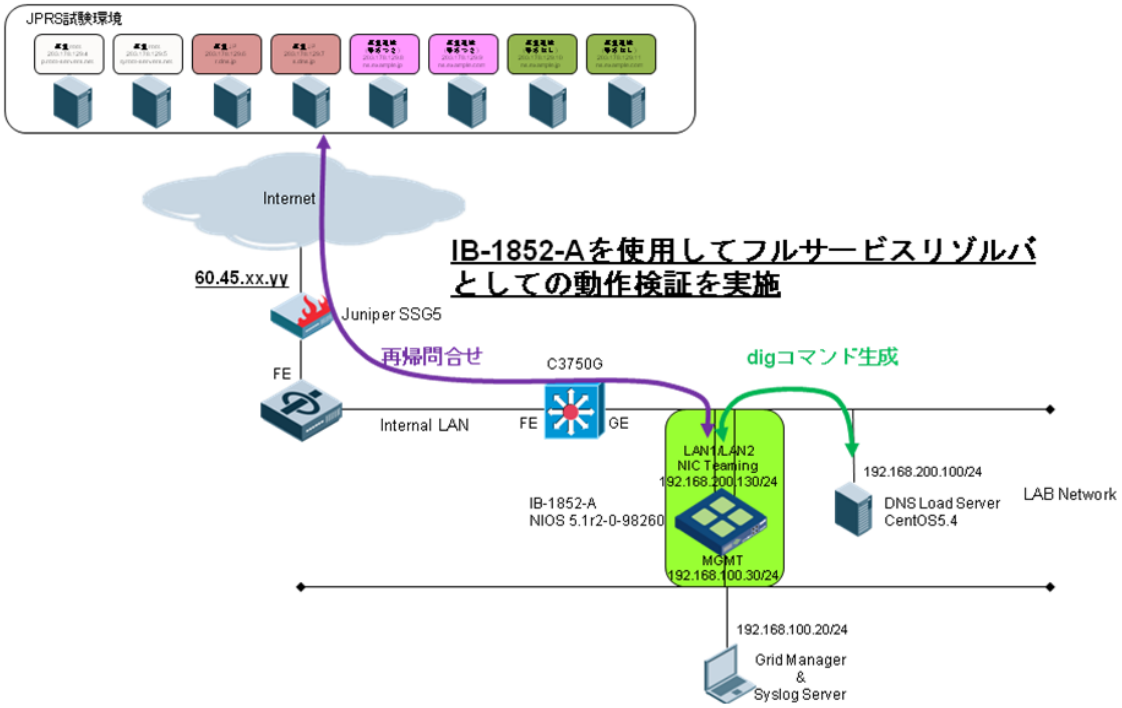
シナリオ 9
①想定した結果とならない
権威サーバ試験にて充当

②権威サーバへの結果は正しいが、フルリゾルバを介すと異常
実施 → 問題なし

■ 事例 4 得られた知見
フルリゾルバにおける問い合わせ失敗(検証の失敗)については、親側権威サーバ
および 権威サーバ、DS、DNSKEY 等のどこか一か所でも問題がある場合、フルリゾルバ側では一律 SERVFAIL となり原因箇所の特定は困難である。
また､原因箇所を特定したとしても権威サーバ側を確認できなければ SERVFAIL の要因となる問題にたどりつけない可能性がある。
→キャッシュ情報の確認内容/取得した署名情報の手動検証/権威サーバへの確認方法など、
運用フロー、および調査手順を確立する必要がある。

機能確認 事例 5

■ 事例 5 実験環境



DNS アプライアンス機器： Infoblox 1852-A Network Service Appliance

ソフトウェアバージョン： NIOS 5.1r2-0-98260

※NIOS = Infoblox アプライアンスの内部 OS の呼称

■ 事例 5 実験結果概要

DNSSEC 機能確認手順書 v1.2 のⅣ.確認項目 2.フルリゾルバ側の確認項目の試験を実施

▼確認項目 F-2. DNSSEC 対応フルリゾルバの利用による AD ビットの確認

－結果 ○

▼確認項目 F-27. RRSIG レコードの有効期間終了フィールドが現在時刻より後であること

－結果 ○

▼確認項目 F-28. RRSIG レコードの有効期間開始フィールドが現在時刻より前であること

－結果 ○

▼確認項目 F-47. DS レコードのアルゴリズムは対応する DNSKEY レコードのものに一致するべき

－結果 ○

▼確認項目 F-49. DS レコードのダイジェストは対応する DNSKEY レコードの鍵のハッシュであるべき

－結果　○

▼確認項目 F-85. セキュリティ対応フルリゾルバは EDNS0 による UDP 通信が可能であること

－結果　○

▼確認項目 F-86. セキュリティ対応フルリゾルバは 1220 バイトの UDP メッセージをサポートしていること

－結果　○

▼確認項目 F-87. セキュリティ対応フルリゾルバは 4000 バイトの UDP メッセージをサポートすべき

－結果　○

▼確認項目 F-130. セキュリティ対応フルリゾルバは元の問い合わせの DO ビットに関わらず、再帰検索においては DO ビットを設定していること

－結果　○

▼確認項目 F-147. セキュリティ対応フルリゾルバの IP 層は IPv4 か v6 かに関わらず、フラグメントされた UDP パケットを正しく処理できなければならない

－結果　○

▼確認項目 F-154. セキュリティ対応フルリゾルバは少なくとも 1 つの信頼できる公開鍵または DS を設定に組み込める機能を持たねばならない

－結果　○

▼確認項目 F-194. 自分自身で署名され REVOKE bit の立った DNSKEY は Revoke される

－結果　今回の技術実験では未試験

▼確認項目 F-196. Revoke された DNSKEY は trust anchor として使用されない

－結果　今回の技術実験では未試験

▼確認項目 F-201. タイマー期限が過ぎたら新しい鍵は trust anchor に追加されること

－結果　今回の技術実験では未試験

▼確認項目 F-202. タイマー期限が来る前に新しい鍵は trust anchor に追加されていないこと

－結果　今回の技術実験では未試験

※補足　F-194、F-196、F-201、F-202 確認項目について

NIOS 5.1r2-0-98260 では RFC5011Automated Updates of DNS Security (DNSSEC) Trust Anchors を未サポートとなっており、今後の NIOS リリースでサポートする予定

▼確認項目 F-229. ゾーンの頂点に NSEC3PARAM レコードが存在すること。

－結果　○

■ 事例 5 実験結果詳細

検証結果詳細

▼確認項目 F-2. DNSSEC 対応フルリゾルバの利用による AD ビットの確認

```
[root@centos ~]# dig +dnssec @192.168.200.130 www.jprs.jp a
```

```
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 www.jprs.jp
a
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14593
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.jprs.jp.                   IN      A

;; ANSWER SECTION:
www.jprs.jp.            900     IN      A       192.0.2.1
www.jprs.jp.            900     IN      RRSIG   A 8 3 900 20101225232004 20091225222004
14883 jprs.jp. VizFF1EuRocTXsrACbU52G5YQi8CQEhxzwFrSoHgv8+PqXeXD3jhXsqe
KXtZQIzUEYKVMghjs/CkOLeLG7wOV4z2oKhkQ7OTVTVc/Qqq8fnpQh5Z
B3TytXng3ZkO25UcbH6ujw4clYSCTKGexn3ia4tm1XCuGb2xDUOhPsc+ SyO=

;; Query time: 151 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 15:43:51 2010
;; MSG SIZE  rcvd: 223
```

▼確認項目 F-27.RRSIG レコードの有効期間終了フィールドが現在時刻より後であること

▼確認項目 F-28.RRSIG レコードの有効期間開始フィールドが現在時刻より前であること

```
[root@centos ~]# dig +dnssec @192.168.200.130 jprs.jp SOA

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 jprs.jp SOA
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50086
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;jprs.jp.                        IN      SOA

;; ANSWER SECTION:
jprs.jp.                900     IN      SOA     ns.jprs.jp. root.jprs.jp. 1 3600 900
604800 900
jprs.jp.                900     IN      RRSIG   SOA 8 2 900 20101225232004
20091225222004 14883 jprs.jp. EDXMyT8SJMbntpEHLRNMO37GzpVONWFjkTVWJVbEW2SOPzMFNaeyERD2
WnrlRaDq11xYYDSotg1lsmSFSTICJmS1g2iFS3KTDU2MSTQH/qjZjlyd
wNC/oWYnXLtollhJRD+Afg4BgEwQ9Yif9KCwf/VrpRj4rOpoKTS+llsx Nzl=
;; Query time: 19 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 16:03:19 2010
;; MSG SIZE  rcvd: 247
```

▼確認項目 F-47. DS レコードのアルゴリズムは対応する DNSKEY レコードのものに一致するべき

▼確認項目 F-49. DS レコードのダイジェストは対応する DNSKEY レコードの鍵のハッシュであるべき

```
[root@centos ~]# dig +dnssec @192.168.200.130 secure.crisp.jp DNSKEY

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130
secure.crisp.jp DNSKEY
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29418
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;secure.crisp.jp.                IN      DNSKEY

;; ANSWER SECTION:
secure.crisp.jp.        3600    IN      DNSKEY  256 3 8
```

```
AwEAAfGAwdnb94WE8rST4J23LOqirOgOekeITguDf+XuAeJG/lXT33k7
lsHeUREhlc98snoTjeOkWLYALaR1f+P5XfSUEkX8+hqNACVb+9s/2ZHD
QzYTHoBd9GSOViEJCSagD1DqF3/XsfHqQ8Qu2w3uEplK1SDz2Vt3m3HD
mGk1goOSQzTq5xFW3xnlebvRzGlBELQnrLww89bvOYGdtycdTcQ/25NI
6d8C76BBpVJHw4CohxPlxkDgR5BCglBkWtx2O8LI8tdBAsFPNp7KuaAr
csm/E5I6plQbi1PKLCuFp1ntOnZMprnPwo3feO6ixNzovjogVfTMt5GM 9DpKAenW1Hk=
secure.crisp.jp.        3600    IN      DNSKEY  257 3 8
AwEAAbbVykYDNiGzdhCaUYN74unlJUMOa6T8dj1lvaCUGXc88SHJqYno
jp7BU+GSjFvC1/GOAZ8tQ/jiT2zbz5uUEg32OdC/SsX2gmzC4lqTLTOZ
44fQo/Ap3vSr9EDlPxES4o5G1TO42SPheBZwY7nb7lQSRlNSflotsOpM
7rgS4SOl8c/HfRc/VGgBq4DJ6GmcP+H73GD8baR95CmwVAxUAvPEtiB9
jkKxEOhxRxUXziAXfA2fTOO5m6AAW/yqtyu1qvmSgnvDKswu2aFbEFVh
864zjE6yEqj3Si8xhlrYJFt/+qdvDZ5XPLR4FqbBO4HsXiPqp4hTYpKs kBt+21VqUxM=
secure.crisp.jp.        3600    IN      DNSKEY  257 3 8
AwEAAd1byrZ98iVpSts+jsCmw2oUCazrjml3N8mDuf7r2QyhX8FeDTIC
O47gCxY4vgM37wPU772wuKuINPOzAAU3HPbblYpaHYqkAavjNv6balij
kZbgaGoclXmQnDWuwLoZW8EBpkDcURx6zltaMoJdrD6w+VJOgCRkEJ35
Zhbyat2hxysnHUiHjrAOgXv2tq8FgemZP7wel68YmHe9l96OuSGjS6Yy
K9zLolTcJ8F3DV1HzgjLsfThRnqvv/DoiGRJKGQ5pvG1SzzgCcsOTmZV
VOfuVSzKAc/moiH3vJkpKH3ZbqZEq/sup9heVYwIl87TQfBqnSObYoZ8 bW+teSV46pO=
secure.crisp.jp.        3600    IN      RRSIG   DNSKEY 8 3 3600 20100913170201
20100816170201 41014 secure.crisp.jp.
bJNzsVuMERTq6DyOLZeoji5SQDjiKC57sOEUOb6SKkTZiAfssznkFoKU
OTEg/QbW5DgOAONgzBRPdLftRdTkL5OzJW3C5ahgZKKRXaG3fycfPNdN
nHvz69AJWQxOlCS/pAbgrg7SUKlanvxAQah5UXFaGR2CTeY8PH+nOjd2
pFZlublutFY9sdxsPDRU4fEQ5LsfpUhCPnC9PL1bETVzcSE5wPOO6UBO
QRZ/z58T5vtOi9h5djfLtnWVHTXSUasSuR6yrU/9dvq+qEUbWJE+szFv
T4H4m3aEcA9jXBhl8Vp1aty8AqMdWgTpqHyFlLyupdCWLH7V+TfzyMvl LS63HQ==
secure.crisp.jp.        3600    IN      RRSIG   DNSKEY 8 3 3600 20100913170201
20100816170201 52567 secure.crisp.jp.
ysdQABVvLHU8jtX+HR8Jnw/rOPFKMoJWqe3DwA3vMlvFqCpVJrS4xFps
klS6G56hXOlfPSJL17bw3T8gQukYQKO6dJuL5Xl7LkmndDWMZpOC5Qgq
JKkJc4mBrOhvsNmgMssHRgs+FlnSkHV9ztLquUSP9lkD5zNtFzu8Ppml
Uc2t3jUVwUfTgUTruAU3o2zHKdtB3glcwD47hfbmEg3C5k88+bPePAY4
jBz/ki3k2clDfXHMOPbzReBQOOiOB2lluA91GtfXwTv7J4bFN7QSVBLS
ev1bSM7Fpz3RZ7lRojLvmWlfnTzqptSHBTL7ahKo8PkXU3m6tqXmRMGw l8BshQ==
secure.crisp.jp.        3600    IN      RRSIG   DNSKEY 8 3 3600 20100913170201
```

```
20100816170201 55533 secure.crisp.jp.
LgGz9nPUF4cZAf/bsBnHrOfXGoXYor79flBxUqCkEwK2gxA8lco2KvdR
dkixWqJR6uq3WDXQq1281sEznbfgXzzkL9AuglbCl9aPPxG9tnKccEf6
VVSLF4XZ54icOHZsOte4c5AJREb4QMktCZ5cdT9BynGl1ixzSL5nDTGe
OCbGHUdCGLK6A6lMaSO5c9sj36z6rYO3bUJc1OBeLQsy7n91ZkbOjHrq
PcXCFviJ8s/drSq7SdJ8zzMHblns3O8pql2NhznVTZf36NOBf5dal6/f
2DU7javf8FqgWo2lBvK/EGpuURed97BoDsXGm5gwQN4pM4r7TqZhcJRJ NCq88g==

;; Query time: 23 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 16:29:21 2010
;; MSG SIZE  rcvd: 1781
```

▼確認項目 F-85. セキュリティ対応フルリゾルバは EDNS0 による UDP 通信が可能であること

▼確認項目 F-86. セキュリティ対応フルリゾルバは 1220 バイトの UDP メッセージをサポートしていること

▼確認項目 F-87. セキュリティ対応フルリゾルバは 4000 バイトの UDP メッセージをサポートすべき

```
[root@centos ~]# dig +dnssec @192.168.200.130 crisp.jp DNSKEY

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 crisp.jp
DNSKEY
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15040
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;crisp.jp.                      IN      DNSKEY

;; ANSWER SECTION:
crisp.jp.               120     IN      DNSKEY  256 3 8
AwEAAarS/K6aW3SzFgYFbXYSIoSfYC4CKP1dEW6/p1SlcwZvsUfiBrzV
i4FGgol1mBnCgy71h5teGNn9MAlqMpXG2fOcGFdSsqO5DRsfPeu1f9Vr
```

「;; Truncated, retrying in TCP mode.」というメッセージが表示されていない

O/YZ21jE/ORZOvrH/iSmp1WhZN9w9rlJcPbNFDTkqMW9DbR4ZVQKiHyD C5uineLt
crisp.jp. 120 IN DNSKEY 256 3 8
AwEAAdCB3QOZ5tVMLjZOlXzh7E2ymjNf5uUUqXXmOkBJN3+J2llGUl18
QoncJxDP4ytGjFsLcmqimfq+PhlpqUyl3YAZnllm+bRFt8fieF/gt3uk
g9H7nA+kb44PuyJmp/iFhzOrA8uq9LkKCD/5VLnrnK+awNs3k8HnPmCr 4ElFSKl3
crisp.jp. 120 IN DNSKEY 257 3 8
AwEAAbQJK+no7FHAm9eeWlF2DAlQBSimcuK8hODj3BDMZS5s4Svv2mxo
e5P5zUtoel3Ewhv2dRfBOznZMUvC6H9gG7lF5h9VDdKmH4O71TL/yycp
2COJ7UOr+xvqJLfMkx2odPRBS4xlK+5xk7XMRcfcwXx34eQTgPUa8+ye
FvRNclzHgOgVA9/N/iZ94wUMSxW1y4YyEONmVtHbVyssU8DAP7yzYc/F
5BEHtXdvxmapQ4LR9V4Z8p7V8rmklL4OJRRB7O8AxWrxM7y4RNHr/6VO
nMRCXT6G1Ee7SqBFAw183juDvlwODjtHPOjOqdoQWpPSe7cNDd16xLAd TlAT3RML2PE=
crisp.jp. 120 IN DNSKEY 257 3 8
AwEAAdtNcWMzNhB6frxTiy/sNltspZlfchONoqUNDx3uP33sslxGgdKs
3W2hSpweK6PwMW/hFiyYwbnfrHK3pmZlP6PylH1femxtLyU2ozvAYUD5
U4g5eo71YteyOxNaBlFAuMUXGm2KZjUeuN/2lS2iZjQEYYa/ew1st4sd
ZRztjB/euTz1lsffMap5CqiJQyS6Awc84LwafYzFxTs93MnuoNoqp9lM
G/wM6BvEqMvkC5HOAgsL+vxM/BuxcFdXOlug29weV92uKO2cZUwtct81
+z1Ld/E7kQhtnVZOZRFrq4CDuYsBJPwm1rec8E4WX91UkPWaMOqHDmOW doe+OQMWqbc=
crisp.jp. 120 IN RRSIG DNSKEY 8 2 120 20100901104857
20100802104857 10770 crisp.jp. jnhD5yy42Qew3Vd/Ee4fQuQNx6pLrJcknpRREtoqGOfwY8xZf3+WtqUy
RwkOe53i4+1Etml+4LeL4dscf159vlEWMwwMAXn9bdL/no2yBapeqfoK
rfbMrSNCHTgPtHX63CGj1riEqx/MltDPxZiG6yvG/RKehztySj8cNW8V 9Jg=
crisp.jp. 120 IN RRSIG DNSKEY 8 2 120 20100901104857
20100802104857 42817 crisp.jp. CLg1CCTll5U5rXMxYc7YECDwROuaGsHw/zlnojz19rVsZlUxes7s6QlR
ToZ2Jvhur7NiyXcwFs8uCWhVB4oSKVgPwnWE2bUhOL7vRfmJdsKSy3Jv
m56xYxiTu/8QN9YsxXjg+bDgTKrxAJoZJX1nQHhOUmLKOWa+M9vgPezZ
jZOfLVMvElenOArzaVmVh2wv4OqCci/HAivrDpWmkNBNrFlscgusMOzd
/tawQhl5N42q+GrYU1giKQq3NH8bpLSFLqWrVWK+5q2Ti1J/pmX39WOe
oyzq6Ou/KSwGKaK3ebTO+hyyd3HQ8ZkZqolZXEWfYsVcgSlcpGXL2lux 88x+Gg==
crisp.jp. 120 IN RRSIG DNSKEY 8 2 120 20100901104857
20100802104857 46627 crisp.jp. ZZTAtUpOUJ4CfLkYZm/4lcC6b6bnR6L+cSaR1fTrh8y5PvC+jbGVZU1P
kYZhdfKO/uillsboULvDl26eAOShy3Di55e8PQlsbA1qLUzbS+KvbpSy
3QaQcdyJ2ZhFfLt2heHSTllYuE/wNMODzElLZG4oGELchNq5clwBnAg2
pjO34HwK41//JMAEFZRg7fueltL7xAes1QEnMFOR7tRQv/WiG5D825WV
elUd16uPqngoOWIiWR/JEVCMfaxpq87rP8kgSu7HDlLAzMT7W6DqO9Pj
GP+Y9lyFYwL7wxWMvHeG6zOjBzTDzDnDlRa/LJmlvoq4UMuBCJC/R3Ze Rz28/Q==

```
;; Query time: 22 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 16:44:01 2010
;; MSG SIZE  rcvd: 1645
```

▼確認項目 F-130. セキュリティ対応フルリゾルバは元の問い合わせの DO ビットに関わらず、再帰検索においては DO ビットを設定していること

```
[root@centos ~]# dig @192.168.200.130 www.jprs.jp A

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> @192.168.200.130 www.jprs.jp A
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1864
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.jprs.jp.                   IN      A

;; ANSWER SECTION:
www.jprs.jp.            900     IN      A       192.0.2.1

;; Query time: 868 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 17:02:34 2010
;; MSG SIZE  rcvd: 45
```

キャッシュの中身の確認

```
Infoblox > set dns flush all
Infoblox > show dns cache
;
; Start view default
;
;
; Cache dump of view 'default' (cache _default)
;
$DATE 20100817080328
```

```
; secure
.                       86345   IN NS   p.root-servers.net.
                        86345   IN NS   q.root-servers.net.
; secure
                          86345   RRSIG   NS 8 0 86400 20110712091518 (
                                          20100712081518 40509 .
                                          U5lmzncDTyS3Up+rdFZnlV+gPw1KAlhtv5Fb
                                          CtR7VyAvYWP529nfO8+pKC6tBqZUlWSLElNE
                                          66o7LfBnovzobYNpuqaCUQcXWndFW1VZOM+i
                                          oGpUazpJowpcScJ15Xtbm5h9DN5+9Wa2YQnM
Fyzz8fPPVgpDkyUAMOPQbMk/Oe8= )
～略～
; glue
ns.jprs.jp.             86345   A       203.178.129.8
; pending-additional
                        845     RRSIG   A 8 3 900 20101225232004 (
                                          20091225222004 14883 jprs.jp.
                                          vLk2grQhX9z29iZQE6+xkbZy4JSdDbe5e2Zz
                                          WOn3HKVhOYvwspKodWctgRTvLBuy9Mdl/eBB
                                          rv521NiosZnuXO/cuq/tDbjKxuxj7sdMMVr+
                                          cXdoQzHuhSA4lTuiC+Vn96Eu9wXyw5yjP2Ap
                                          R8am3j71+v9/SiKh4WH9KPwFotO= )
; glue
                          86345   AAAA    2001:200:132:3::8
; pending-additional
                          845     RRSIG   AAAA 8 3 900 20101225232004 (
                                          20091225222004 14883 jprs.jp.
                                          hVnPup5vUGOlJlMlJgJblQLTZidfc1r1215n
                                          cO4PHFeX73NtMRqnxzV39JEJBarN2pAwjTto
                                          9KBZ/ETvp2/5QCMfSa8sHlex1Reew9sRtqBC
                                          iDr/D8rVn7WeDgUF9xY7Mrb616bMrcqMLyBY
                                          j7xsJTqTHNrRnGWxefcROuBO5lO= )
; secure
www.jprs.jp.            846     A       192.0.2.1
; secure
                          846     RRSIG   A 8 3 900 20101225232004 (
                                          20091225222004 14883 jprs.jp.
```

```
                                        VizFF1EuRocTXsrACbU52G5YQi8CQEhxzwFr
                                        SoHgv8+PqXeXD3jhXsqeKXtZQIzUEYKVMghj
                                        s/CkOLeLG7wOV4z2oKhkQ7OTVTVc/Qqq8fnp
                                        Qh5ZB3TytXng3ZkO25UcbH6ujw4clYSCTKGe
                                        xn3ia4tm1XCuGb2xDUOhPsc+SyO= )
～略～
; Bad cache
;
; Dump complete
```

▼確認項目 F-147. セキュリティ対応フルリゾルバの IP 層は IPv4 か v6 かに関わらず、フラグメントされた UDP パケットを正しく処理できなければならない

```
Infoblox > ping  203.178.129.26 packetsize 1472
pinging 203.178.129.26
PING 203.178.129.26 (203.178.129.26) 1472(1500) bytes of data.
1480 bytes from 203.178.129.26: icmp_seq=1 ttl=51 time=12.9 ms
1480 bytes from 203.178.129.26: icmp_seq=2 ttl=51 time=12.2 ms
1480 bytes from 203.178.129.26: icmp_seq=3 ttl=51 time=12.9 ms
1480 bytes from 203.178.129.26: icmp_seq=4 ttl=51 time=12.6 ms
1480 bytes from 203.178.129.26: icmp_seq=5 ttl=51 time=12.6 ms

--- 203.178.129.26 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4019ms
rtt min/avg/max/mdev = 12.282/12.695/12.968/0.250 ms

[root@centos ~]# dig +dnssec @192.168.200.130 crisp.jp DNSKEY

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130 crisp.jp
DNSKEY
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15054
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
```

```
;crisp.jp.                      IN      DNSKEY

;; ANSWER SECTION:
crisp.jp.               8       IN      DNSKEY  256 3 8
AwEAAarS/K6aW3SzFgYFbXYSIoSfYC4CKP1dEW6/p1SlcwZvsUfiBrzV
i4FGgol1mBnCgy71h5teGNn9MAlqMpXG2fOcGFdSsqO5DRsfPeu1f9Vr
O/YZ21jE/ORZOvrH/iSmp1WhZN9w9rlJcPbNFDTkqMW9DbR4ZVQKiHyD C5uineLt
crisp.jp.               8       IN      DNSKEY  256 3 8
AwEAAdCB3QOZ5tVMLjZOlXzh7E2ymjNf5uUUqXXmOkBJN3+J2llGUl18
QoncJxDP4ytGjFsLcmqimfq+PhlpqUyl3YAZnllm+bRFt8fieF/gt3uk
g9H7nA+kb44PuyJmp/iFhzOrA8uq9LkKCD/5VLnrnK+awNs3k8HnPmCr 4ElFSKl3
crisp.jp.               8       IN      DNSKEY  257 3 8
AwEAAbQJK+no7FHAm9eeWlF2DAlQBSimcuK8hODj3BDMZS5s4Svv2mxo
e5P5zUtoel3Ewhv2dRfBOznZMUvC6H9gG7lF5h9VDdKmH4O71TL/yycp
2COJ7UOr+xvqJLfMkx2odPRBS4xlK+5xk7XMRcfcwXx34eQTgPUa8+ye
FvRNclzHgOgVA9/N/iZ94wUMSxW1y4YyEONmVtHbVyssU8DAP7yzYc/F
5BEHtXdvxmapQ4LR9V4Z8p7V8rmkIL40JRRB7O8AxWrxM7y4RNHr/6VO
nMRCXT6G1Ee7SqBFAw183juDvlwODjtHPOjOqdoQWpPSe7cNDd16xLAd TlAT3RML2PE=
crisp.jp.               8       IN      DNSKEY  257 3 8
AwEAAdtNcWMzNhB6frxTiy/sNltspZlfchONoqUNDx3uP33sslxGgdKs
3W2hSpweK6PwMW/hFiyYwbnfrHK3pmZlP6PylH1femxtLyU2ozvAYUD5
U4g5eo71YteyOxNaBlFAuMUXGm2KZjUeuN/2lS2iZjQEYYa/ew1st4sd
ZRztjB/euTz1lsffMap5CqiJQyS6Awc84LwafYzFxTs93MnuoNoqp9lM
G/wM6BvEqMvkC5HOAgsL+vxM/BuxcFdXOlug29weV92uKO2cZUwtct81
+z1Ld/E7kQhtnVZOZRFrq4CDuYsBJPwm1rec8E4WX91UkPWaMOqHDmOW doe+OQMWqbc=
crisp.jp.               8       IN      RRSIG   DNSKEY 8 2 120 20100901104857
20100802104857 10770 crisp.jp. jnhD5yy42Qew3Vd/Ee4fQuQNx6pLrJcknpRREtoqGOfwY8xZf3+WtqUy
RwkOe53i4+1Etml+4LeL4dscf159vlEWMwwMAXn9bdL/no2yBapeqfoK
rfbMrSNCHTgPtHX63CGj1riEqx/MltDPxZiG6yvG/RKehztySj8cNW8V 9Jg=
crisp.jp.               8       IN      RRSIG   DNSKEY 8 2 120 20100901104857
20100802104857 42817 crisp.jp. CLg1CCTll5U5rXMxYc7YECDwROuaGsHw/zlnojz19rVsZlUxes7s6QlR
ToZ2Jvhur7NiyXcwFs8uCWhVB4oSKVgPwnWE2bUhOL7vRfmJdsKSy3Jv
m56xYxiTu/8QN9YsxXjg+bDgTKrxAJoZJX1nQHhOUmLKOWa+M9vgPezZ
jZOfLVMvElenOArzaVmVh2wv4OqCci/HAivrDpWmkNBNrFlscgusMOzd
/tawQhl5N42q+GrYU1giKQq3NH8bpLSFLqWrVWK+5q2Ti1J/pmX39WOe
oyzq6Ou/KSwGKaK3ebTO+hyyd3HQ8ZkZqolZXEWfYsVcgSlcpGXL2lux 88x+Gg==
crisp.jp.               8       IN      RRSIG   DNSKEY 8 2 120 20100901104857
```

20100802104857 46627 crisp.jp. ZZTAtUpOUJ4CfLkYZm/4IcC6b6bnR6L+cSaR1fTrh8y5PvC+jbGVZU1P
kYZhdfKO/uillsboULvDI26eAOShy3Di55e8PQIsbA1qLUzbS+KvbpSy
3QaQcdyJ2ZhFfLt2heHSTIIYuE/wNMODzEILZG4oGELchNq5clwBnAg2
pjO34HwK41//JMAEFZRg7fueltL7xAes1QEnMFOR7tRQv/WiG5D825WV
elUd16uPqngoOWIiWR/JEVCMfaxpq87rP8kgSu7HDILAzMT7W6DqO9Pj
GP+Y9lyFYwL7wxWMvHeG6zOjBzTDzDnDIRa/LJmIvoq4UMuBCJC/R3Ze Rz28/Q==

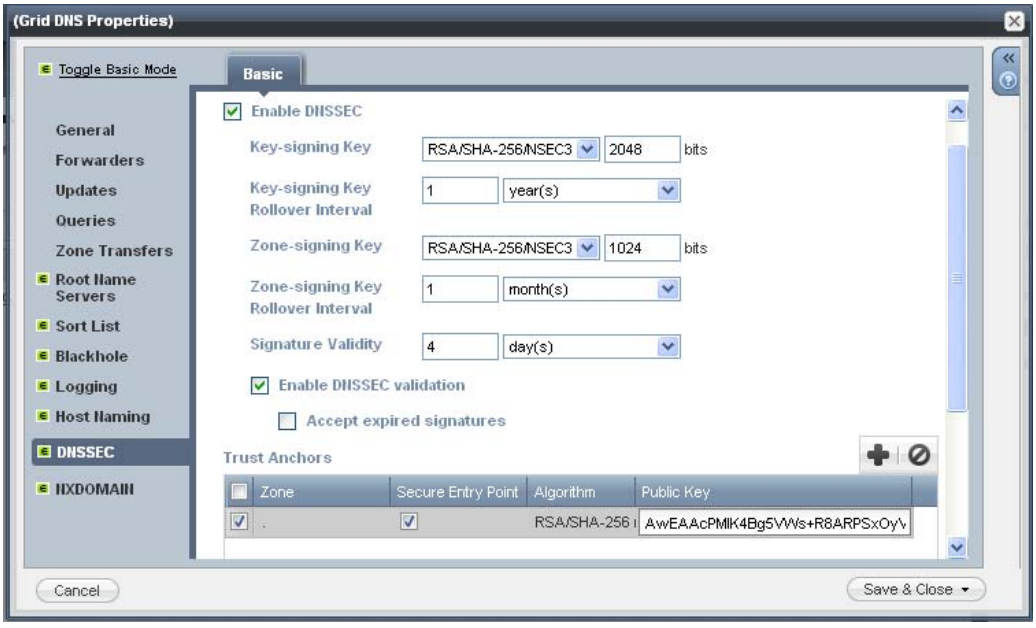
;; Query time: 0 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 17:29:18 2010
;; MSG SIZE rcvd: 1645

▼確認項目 F-154. セキュリティ対応フルリゾルバは少なくとも 1 つの信頼できる公開鍵または DS を設定に組み込める機能を持たねばならない

仮想ツリーのルート鍵

```
trusted-keys {
  "." 257 3 8 "AwEAAcPMIK4Bg5VWs+R8ARPSxOyV+crdg/kawfraPfIT+rCTRdi43MYX
3kG+XJttkVIC5/FEO8yUpjy9dAtSorqOcYXSd66H1UxCq/vwmBEOlpAB
5ODZ/xMgGyp/EOZHvpOgObNo2ITKcggnGmU2KvPYfoXzqH+oyE4ApaE1
2/GZj1AOQQ4nidD23c4FBzpszZXteeiEA8DWkaicfWLKYyjQ75hm4zbu
FvQRq9O6isY+2SVqLiTImzmwWvsf6/onftwOOqToiiUQWvUdMwN6QsjF
/qRamFa7ToPPw37ydSfPWstxiPXj3blWhKOrOZgdr6tEwWtulhD4OWEr Wdqf/bAGZDO=";
};
```

NIOS GUI にて Trust Anchors を設定



▼確認項目 F-194. 自分自身で署名され REVOKE bit の立った DNSKEY は Revoke される

▼確認項目 F-196. Revoke された DNSKEY は trust anchor として使用されない

▼確認項目 F-201. タイマー期限が過ぎたら新しい鍵は trust anchor に追加されること

▼確認項目 F-202. タイマー期限が来る前に新しい鍵は trust anchor に追加されていないこと

F-194,F-196,F-201,F-202 の確認項目については今回の技術実験では未試験

▼確認項目 F-229. ゾーンの頂点に NSEC3PARAM レコードが存在すること。

```
[root@centos bin]# ./dig +dnssec @192.168.200.130 jp NSEC3PARAM

; <<>> DiG 9.6.2-P2 <<>> +dnssec @192.168.200.130 jp NSEC3PARAM
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34689
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;jp.                            IN      NSEC3PARAM

;; ANSWER SECTION:
jp.                     0       IN      NSEC3PARAM 1 0 10 CAFE
jp.                     0       IN      RRSIG   NSEC3PARAM 8 1 0 20100916030235
20100817030235 54813 jp. kEmt4tYBDaH4pUVNl/M++G3q/QTZQLTwk8QEdVleCYTTKAdfA8gxMpvw
tMpcxng2swE65XP5PRNwWRi133Ku4RbCfu1CcgC+7pkC7T6y/SkPNqHf
9NxjAFkGpXGNdigyKaet+JrOV9ItCUmUVL/bs+G8ei5OgGSclJ/HAnel
oxRufg6afqs6ohLzGfeqWK+A7BTCJvbR+mpNr3yeazpBqmg6aX89fb3w
/3sLqUPrOJCkif4+Z1GFiTiv+8vpUiHqZ3uHaj23gCythrhd5r1SBL2Z
QjBvXkLWRUnjN1oVJNs+34L3ZUDoMM3gPtqzqpBMmOuK2hiun5jrYNMA c5p9ng==

;; Query time: 13 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 17 20:37:34 2010
;; MSG SIZE  rcvd: 340
```

■ 事例 5 得られた知見

▼RSA/SHA-2 署名アルゴリズムへの Infoblox NIOS の対応について

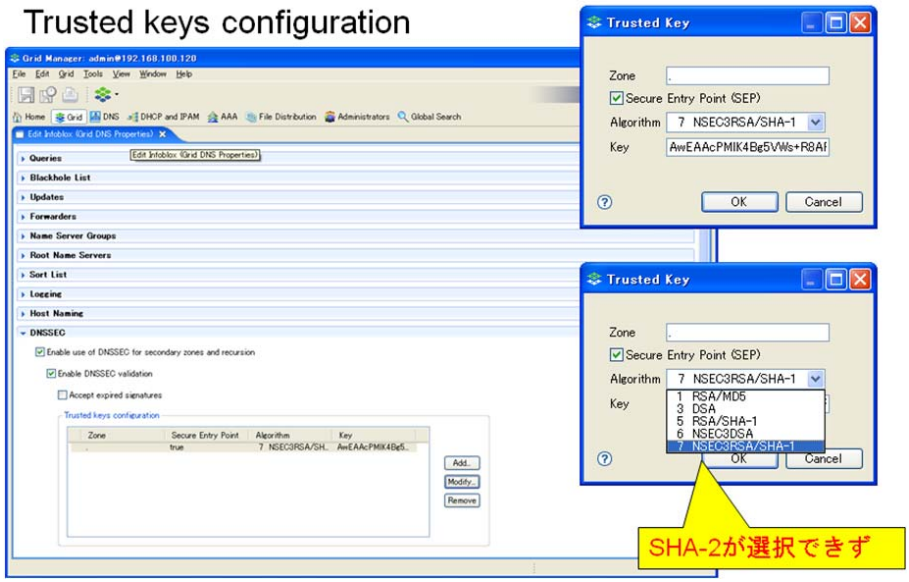
Infoblox NIOS4.3r3 以降のバージョンで DNSSEC ゾーン用セカンダリネームサーバ、キャッシュ（フルサービスリゾルバ）ネームサーバ用トラストアンカーのインポート、NIOS5.0r1 以降のバージョンで DNSSEC ゾーン用プライマリネームサーバの鍵の管理、署名機能をサポートしていますが、Root DNS で使用されている RSA/SHA-2（SHA-256/SHA-512）署名アルゴリズムのサポートは NIOS5.1r2 からとなっております。

今後、Infoblox アプライアンスにて DNSSEC 対応キャッシュネームサーバを展開する場合には、RSA/SHA-2 署名アルゴリズムをサポートする NIOS5.1r2 以降のソフトウェアの導入を推奨いたします。

▼署名アルゴリズムが不一致の場合のキャッシュサーバでの Validation 失敗事例

NIOS4.3r6 での試験結果

仮想ルートサーバは RSA/SHA-2 署名アルゴリズムを使用



キャッシュサーバの DNSSEC Validation をイネーブル化して試験すると以下のように失敗する

```
C:¥dig>dig @192.168.200.120 jprs.jp a +dnssec

; <<>> DiG 9.3.2 <<>> @192.168.200.120 jprs.jp a +dnssec
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 1797
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;jprs.jp.                       IN      A

;; Query time: 187 msec
;; SERVER: 192.168.200.120#53(192.168.200.120)
;; WHEN: Fri May 21 14:07:18 2010
;; MSG SIZE  rcvd: 36
```

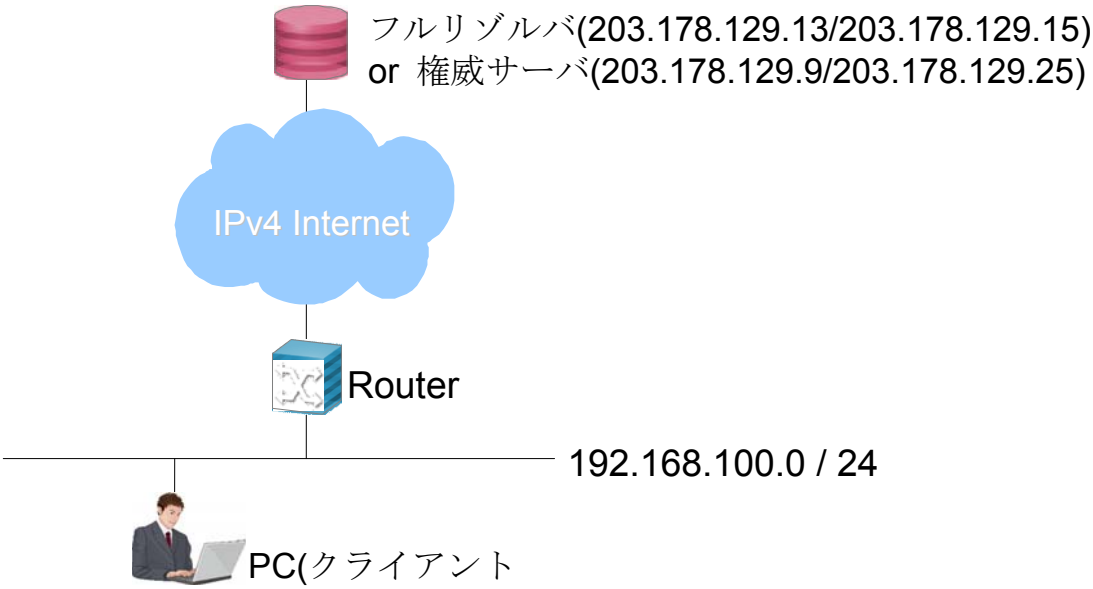
SERVFAILが返る

署名アルゴリズム不一致の為
Validationに失敗

```
May 21 14:11:55 (none) named[23718]: client 192.168.1.23#3712:  query: jprs.jp IN A +ED
May 21 14:11:55 (none) named[23718]: validating @0x85a2258: jprs.jp A: no valid signature found
May 21 14:11:55 (none) named[23718]: validating @0x85b02c8: jp DS: no valid signature found
May 21 14:11:55 (none) named[23718]: no valid RRSIG resolving 'jp/DS/IN': 203.178.129.5#53
May 21 14:11:55 (none) named[23717]: validating @0x85b02c8: jp DS: no valid signature found
May 21 14:11:55 (none) named[23717]: no valid RRSIG resolving 'jp/DS/IN': 203.178.129.4#53
May 21 14:11:55 (none) named[23717]: no valid DS resolving 'jprs.jp/A/IN': 203.178.129.9#53
May 21 14:11:55 (none) named[23717]: validating @0x85ae2b8: jprs.jp A: no valid signature found
May 21 14:11:55 (none) named[23717]: validating @0x85b02c8: jp DS: no valid signature found
May 21 14:11:55 (none) named[23717]: no valid RRSIG resolving 'jp/DS/IN': 203.178.129.4#53
May 21 14:11:55 (none) named[23718]: validating @0x85b02c8: jp DS: no valid signature found
May 21 14:11:55 (none) named[23718]: no valid RRSIG resolving 'jp/DS/IN': 203.178.129.5#53
May 21 14:11:55 (none) named[23718]: no valid DS resolving 'jprs.jp/A/IN': 203.178.129.8#53
```

機能確認 事例 6

■ 事例 6 実験環境



※PC(クライアント)には CentOS5.4 を使用。
BIND-9.7.0rc1 をインストールする。

■ 事例 6 実験結果概要

フルリゾルバもしくは権威サーバそれぞれに対して、さらにそれぞれで署名ありの場合と署名なしの場合について、クライアントからの DNS 要求を必要十分な標準的フィルターを設定したルータがトランスペアレントに転送する接続形態で、以下の確認項目を実施することにより、ルータの振る舞いが DNSSEC の通信の妨げにならないことを確認した。

F-85.セキュリティ対応フルリゾルバは EDNS0 による UDP 通信が可能であること
F-86.セキュリティ対応フルリゾルバは 1220 バイトの UDP メッセージをサポートしていること
F-87.セキュリティ対応フルリゾルバは 4000 バイトの UDP メッセージをサポートすべき
A-85.セキュリティ対応権威サーバは EDNS0 による UDP 通信が可能であること
A-86.セキュリティ対応権威サーバは 1220 バイトの UDP メッセージをサポートしていること
A-87.セキュリティ対応権威サーバは 4000 バイトの UDP メッセージをサポートすべき

■ 事例 6 実験結果詳細

▼フルリゾルバ(署名あり)に問い合わせ

○確認項目 F-85.セキュリティ対応フルリゾルバは EDNS0 による UDP 通信が可能であること。

1.応答結果が 512 バイトを越えるような問い合わせをフルリゾルバに対して行う。

- dig コマンドに+dnssec オプションを付けて問い合わせを行う。
- @の横はフルリゾルバのアドレス。
- 署名付きゾーンのゾーン名を指定する。
- レコードタイプは DNSKEY を指定する。以下について確認する。

以下について確認した。

- ゾーンに対する DNSKEY レコードと RRSIG レコードが応答に含まれていることを確認。
- 応答結果の MSG SIZE rcvd:のデータ量が 512 を越えていることを確認。
- dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていないことを確認。
- 応答結果の OPT PSEUDOSECTION 部の udp が 4096 になっていることを確認。

2.+bufsize=512 オプションを付加して行う。

以下について確認した。

- dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていることを確認。　問い合わせに対するサーバの応答のデータ量が PC から指定した UDP の最大データサイズを超えたため。

○確認項目 F-86.セキュリティ対応フルリゾルバは 1220 バイトの UDP メッセージをサポートしていること。

応答結果が 1220 バイトを越えるような問い合わせをフルリゾルバに対して行う。

以下について確認した。

- ゾーンに対する DNSKEY レコードと RRSIG レコードが応答に含まれていることを確認。
- SIZE rcvd:のデータ量が 1220 を越えていることを確認。
- dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていないことを確認。

○確認項目 F-87.セキュリティ対応フルリゾルバは 4000 バイトの UDP メッセージをサポートすべき

ローカルに別のフルリゾルバ（Fedora10、BIND-9.7.0rc1）を立て、MSG SIZE が 4000 を超えるように設定。
以下について確認した。

・ 応答結果が 4000 バイトを越えるような問い合わせを正常に応答結果が得られることを確認。

▼フルリゾルバ(署名なし)に問い合わせ

○確認項目 F-85.セキュリティ対応フルリゾルバは EDNS0 による UDP 通信が可能であること。

1.応答結果が 512 バイトを越えるような問い合わせをフルリゾルバに対して行う。

・ dig コマンドに+dnssec オプションを付けて問い合わせを行う。
・ @の横はフルリゾルバのアドレス。
・ 署名なしのゾーン名を指定する。
・ レコードタイプは DNSKEY を指定する。以下について確認する。

以下について確認した。

・ ゾーンに対する DNSKEY レコードと RRSIG レコードが応答に含まれていない。
・ dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていないことを確認。
・ 応答結果の OPT PSEUDOSECTION 部の udp が 4096 になっていることを確認。

○確認項目 F-86.セキュリティ対応フルリゾルバは 1220 バイトの UDP メッセージをサポートしていること。

署名がなく MSG SIZE を大きくすることができないため確認できず。

○確認項目 F-87.セキュリティ対応フルリゾルバは 4000 バイトの UDP メッセージをサポートすべき

署名がなく MSG SIZE を大きくすることができないため確認できず。

▼権威サーバ(署名あり)に問い合わせ

○確認項目 A-85.セキュリティ対応権威サーバは EDNS0 による UDP 通信が可能であること。

1.応答結果が 512 バイトを越えるような問い合わせを権威サーバに対して行う。

・ dig コマンドに+dnssec、+norec オプションを付けて問い合わせを行う。
・ @の横は権威サーバのアドレス。
・ 署名付きゾーンのゾーン名を指定する。
・ レコードタイプは DNSKEY を指定する。

以下について確認した。

・ ゾーンに対する DNSKEY レコードと RRSIG レコードが応答に含まれていることを確認。
・ 応答結果の MSG SIZE rcvd:のデータ量が 512 を越えていることを確認。
・ dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていないことを確認。
・ 応答結果の OPT PSEUDOSECTION 部の udp が 4096 になっていることを確認。

2.+bufsize=512 オプションを付加して行う。

以下について確認した。

・ dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていることを確認。　問い合わせに対するサーバの応答のデータ量が PC から指定した UDP の最大データサイズを超えたため。

○確認項目 A-86.セキュリティ対応権威サーバは 1220 バイトの UDP メッセージをサポートしていること。

応答結果が 1220 バイトを越えるような問い合わせを権威サーバに対して行う。

以下について確認した。

・ ゾーンに対する DNSKEY レコードと RRSIG レコードが応答に含まれていることを確認。
・ 応答結果の MSG SIZE rcvd:のデータ量が 1220 を越えていることを確認。
・ dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていないことを確認。

○確認項目 A-87.セキュリティ対応権威サーバは 4000 バイトの UDP メッセージをサポートすべき

ローカルに別の権威サーバを立てないと実施できなかったため確認できず。

▼権威サーバ(署名なし)に問い合わせ

○確認項目 A-85.セキュリティ対応権威サーバは EDNS0 による UDP 通信が可能であること。

1.応答結果が 512 バイトを越えるような問い合わせを権威サーバに対して行う。

- dig コマンドに+dnssec、+norec オプションを付けて問い合わせを行う。
- @の横は権威サーバのアドレス。
- 権威あるゾーンのゾーン名を指定する。
- レコードタイプは DNSKEY を指定する。

以下について確認した。

- ゾーンに対する DNSKEY レコードと RRSIG レコードが応答に含まれていない。
- dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていないことを確認。
- 応答結果の OPT PSEUDOSECTION 部の udp が 4096 になっていることを確認。

2.+bufsize=512 オプションを付加して行う。

以下について確認した。

- dig コマンドの実行結果のすぐ下に「;; Truncated, retrying in TCP mode」が表示されていることを確認。　問い合わせに対するサーバの応答のデータ量が PC から指定した UDP の最大データサイズを超えたため。

○確認項目 A-86.セキュリティ対応権威サーバは 1220 バイトの UDP メッセージをサポートしていること。

署名がなく MSG SIZE を大きくすることができないため確認できず。

○確認項目 A-87.セキュリティ対応権威サーバは 4000 バイトの UDP メッセージをサポートすべき。

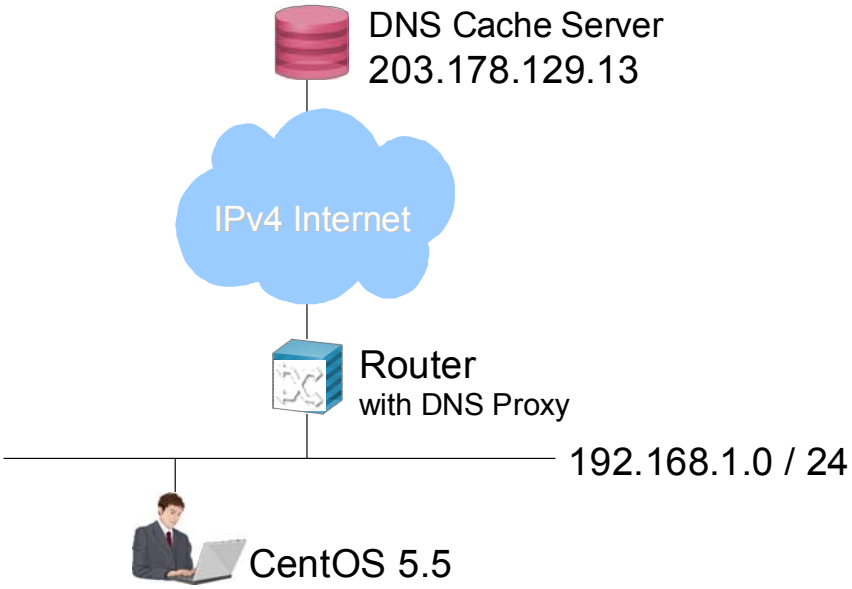
署名がなく MSG SIZE を大きくすることができないため確認できず。

■ 事例 6 得られた知見

一部実施できなかった項目はあったが、ルータのフィルター機能および転送機能はフルリゾルバならびに権威サーバに対する DNSSEC の通信を、署名のあるなしにかかわらず、妨げないことが概ねわかった。

機能確認 事例 7

■ 事例 7 実験環境



■ 事例 7 実験結果概要

DNSSEC 機能確認手順書の F-85、F-86、F-87 および [RFC5625] DNS Proxy Implementation Guidelines を参考情報と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 機能の検証を行った。

■ 事例 7 実験結果詳細

（1）OPT RR や 各種 Flags を透過的に処理しているか確認を実施。

→ 全機種において正常性を確認した。

（2）EDNS0 に対応し、1,220 bytes の Packet を適切に処理できるか確認を実施した。

→ 一部機種において適切に処理していないことを確認した。

（3）EDNS0 に対応し、4,000 bytes の Packet を適切に処理できるか確認を実施した。

→ 一部機種において適切に処理していないことを確認した。

（4）TCP Fallback が適切に機能しているか確認を実施した。

→ 一部機種において適切に機能していないことを確認した。

（5）DNS Cache 有無による影響を確認した。

→ 一部機種において Cache 有りが悪影響を及ぼしていることを確認した。

■ 事例 7 得られた知見

一部機種において 512byte 以上の Packet を適切に処理できないこと、特定 RR の Cache のみを行う実装の場合、DNSSEC 検証を実施できない条件があることを確認した。

Cache 機能を実装する場合、特定 RR だけでなく全ての RR を Cache することが望ましいが、考慮事項が多い為、Cache 機能を実装しないことが現実解であると考える。

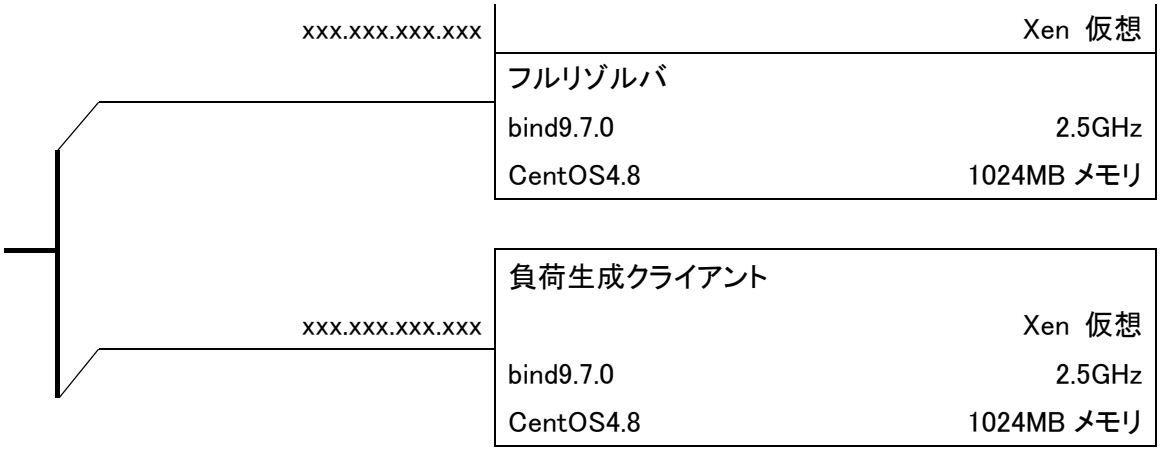
（1）512byte 以上の Packet を適切に処理できない問題。
512byte 以上の応答 Packet 受信時、512byte に切り詰めて転送を行っているが、TC＝0 で転送している為、スタブリゾルバでは TCP Fallback を行うこともできない。

（2）特定 RR のみを Cache する実装の問題。
特定 RR のみを Cache する実装では、RRSIG RR が Cache されない実装となっていた。この状態で別端末からの問合せ等が行われた場合に Cache した RR のみを応答する為、Cache Entry が無くなる（TTL 満了）までの間は DNSSEC 検証を行うことができない。

性能確認結果

性能確認　事例 1

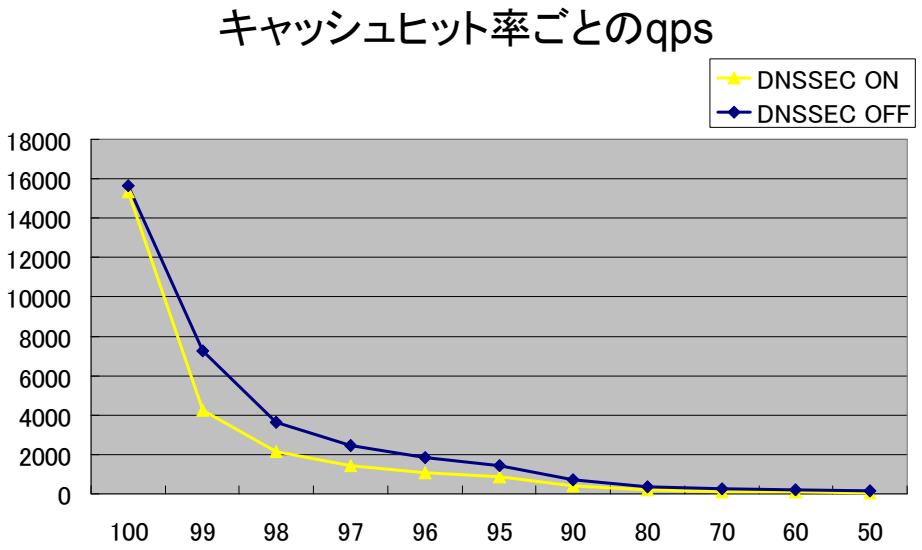
■ 事例 1　実験環境

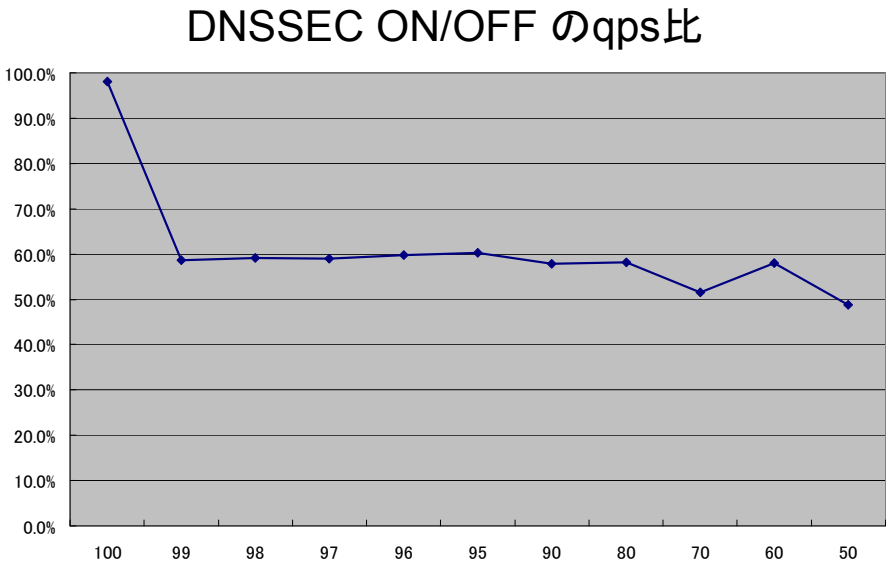


■ 事例 1　実験結果概要

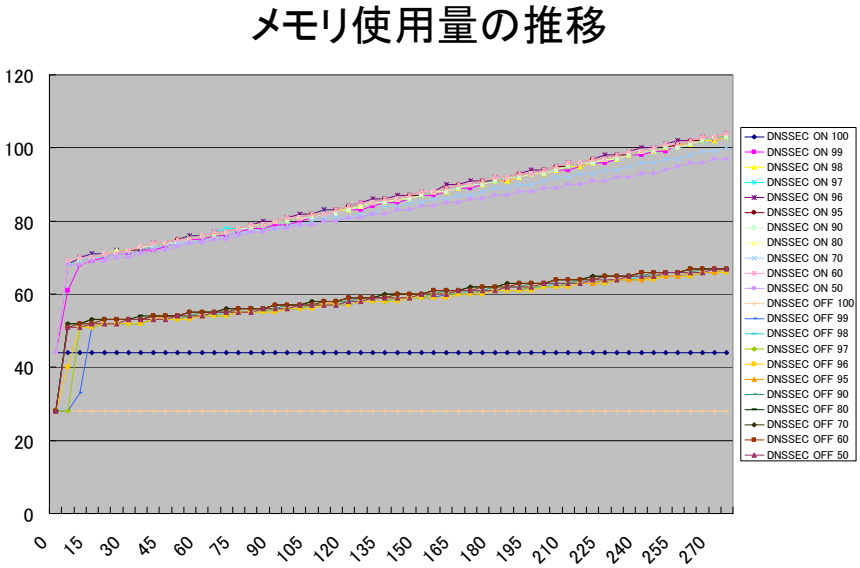
DNSSEC を有効にすることにより、フルリゾルバでの CPU 使用率上昇、メモリ使用量の増加、クエリ処理性能の低下が確認できた。

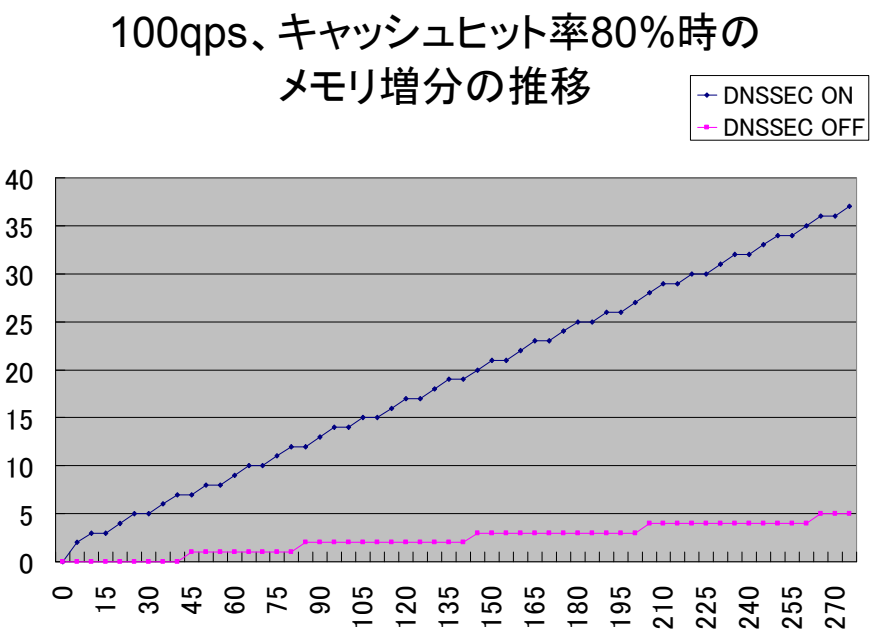
■ 事例 1　実験結果詳細（1）




DNSSEC ON/OFF のqps比
100.0%
90.0%
80.0%
70.0%
60.0%
50.0%
40.0%
30.0%
20.0%
10.0%
0.0%
100
99
98
97
96
95
90
80
70
60
50

■ 事例 1 実験結果詳細（2）


メモリ使用量の推移
120
100
80
60
40
20
0
0
15
30
45
60
75
90
105
120
135
150
165
180
195
210
225
240
255
270
DNSSEC ON 100
DNSSEC ON 99
DNSSEC ON 98
DNSSEC ON 97
DNSSEC ON 96
DNSSEC ON 95
DNSSEC ON 90
DNSSEC ON 80
DNSSEC ON 70
DNSSEC ON 60
DNSSEC ON 50
DNSSEC OFF 100
DNSSEC OFF 99
DNSSEC OFF 98
DNSSEC OFF 97
DNSSEC OFF 96
DNSSEC OFF 95
DNSSEC OFF 90
DNSSEC OFF 80
DNSSEC OFF 70
DNSSEC OFF 60
DNSSEC OFF 50



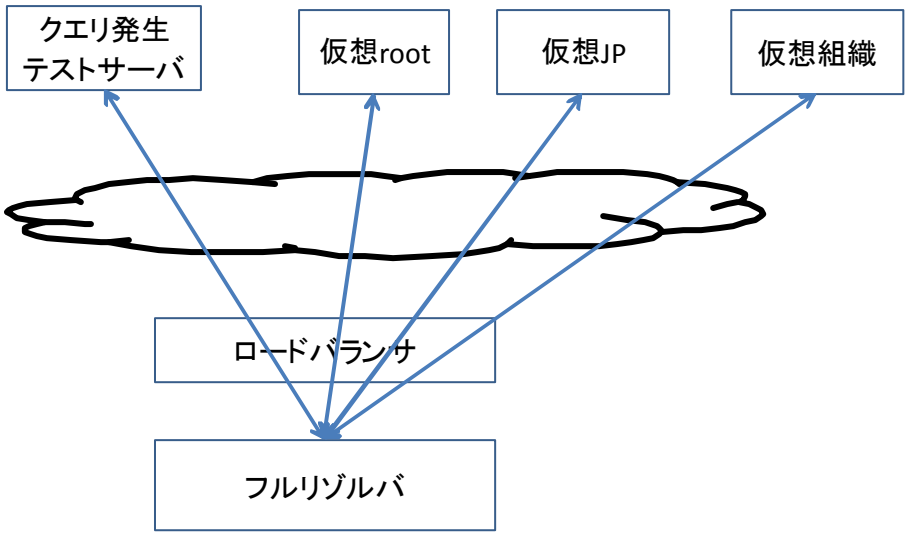
■ 事例 1 得られた知見

NSEC3 使用、クエリがほぼ NXDOMAIN の状態ではメモリ使用量が 8 倍になった。

DNSSEC ON 時は、OFF 時に比べクエリ処理能力が 60%程度に低下した。

性能確認 事例 2

■ 事例 2 実験環境



機能	HW	アプリケーション	備考
フルリゾルバ	SUN X2100 Solaris10	bind-9.7.0	IPv4 のみ
ロードバランサ	A10networks AX2500		IPv4 のみ
クエリ発生	SUN NetraT1	queryperf 改造版	IPv4 のみ

■ 事例 2 実験結果概要

JPRS 提供の DNSSEC 性能確認手順書 Ver. 1.1 の 5.計測手順のうち以下についてキャッシュサーバで実験実施

５．計測手順

５． １．Validator の各パターンによる挙動変化の計測

a) dig による DNS 名前解決と、DNSSEC 検証の確認

1. パターンによって、以下の設定を変更する。

・Validator サーバのネットワーク設定を変更する。(MTU, TCP, フラグメント)

・Validator サーバの設定ファイルを変更する。(DO=0/1, TA の設定)

・権威サーバに設定するゾーンデータを変更する。(ZSK=1024/2048, 署名なし)

2. 上記の設定後、Validator および権威サーバが起動している状態で、
Validator サーバ上で dig により下記の例にあるコマンドにて確認を行う。
dig の出力結果をみて、名前解決の成否・検証の成否を確かめる。

署名無しの場合

dig @localhost example.jp. A

署名ありの場合

dig @localhost +dnssec example.jp. A

b) 名前解決ができるパターンに対し、Validator の負荷と権威サーバへのクエリ内容を計測する。

1. パターンによって、a)と同様にネットワークおよびサーバの設定を変更する。
2. Validator サーバ上で、負荷計測ツール(※)を起動し CPU 使用率およびメモリ使用量の計測を開始する。

※ CPU 使用率、メモリ使用量、ロードアベレージなどを計測するスクリプトを用意する。

3. Validator および権威サーバ上で、DSC(DSC Collector)を稼動させる。
4. クエリ発生機上で queryperf(改造版)による負荷テストを行う。DO ビットによってコマンドを使い分ける。

-i オプションに送信間隔をミリ秒単位で指定する。下記の例では 0.1ms なので 10000qps で送信する。

DO=0

queryperf -d query.txt -s 192.0.2.1 -l 300 -i 0.1

DO=1

queryperf -d query.txt -s 192.0.2.1 -D -l 300 -i 0.1

5. 負荷を掛け終わったら、Validator および権威サーバで起動した負荷計測ツール/DSC を終了させる。

上記手順において、検証および計測の間でのパターンの切り替えは以下のように行う。

■ 事例 2 実験結果詳細

計測手順のうち ５．１． の a) の １． について

・MTU、TCP、フラグメント等のネットワーク設定変更については、実験環境が本番環境と同居しているため変更不可であったため未実施。

・Validator の設定ファイル変更については、TA の設定有無による挙動変化をみた

・権威サーバは構築していないため未実施。

計測手順のうち ５．１． の b) について

queryperf にて 5 分間継続してキャッシュヒットしないようなテストクエリを用意することができなかった。

よってしばらくするとキャッシュヒット(と思われる)により署名検証によるサーバへの負荷が想定よりも低いものとなり、署名検証の有無によるサーバへの負荷に顕著な違いは見られなかった。

ただし、キャッシュサイズについては、署名無し仮想ツリーへのアクセス時と署名有り仮想ツリーへのアクセス時では、2 倍以上の差が確認できた。

■ 事例 2 得られた知見

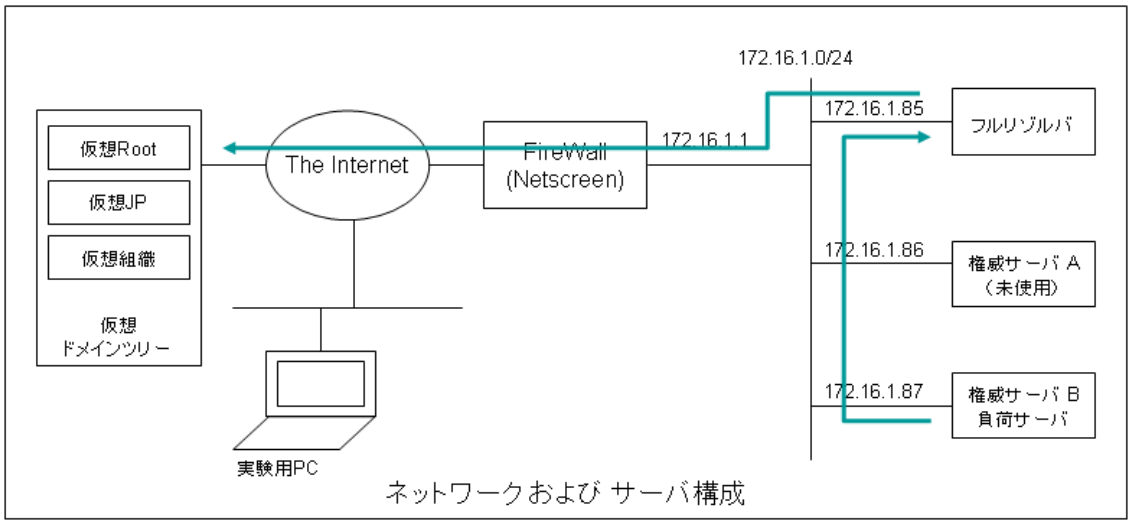
負荷状況については DNSSECON/OFF による顕著な違いをみることはできなかった。

ただ、キャッシュサイズについては 2 倍以上になることが見込まれるため、サービス環境内のサーバの負荷、処理能力を鑑みたうえでサーバのリプレース等を適宜実施する必要があると思われる。

性能確認 事例 3

■ 事例 3 実験環境

・実験環境構成



・ソフトウェア構成

OS：Solaris10　BIND：9.7.0-P1

・負荷ツール

queryperf　dnsperf

■ 事例 3 実験結果概要

<実験手順>

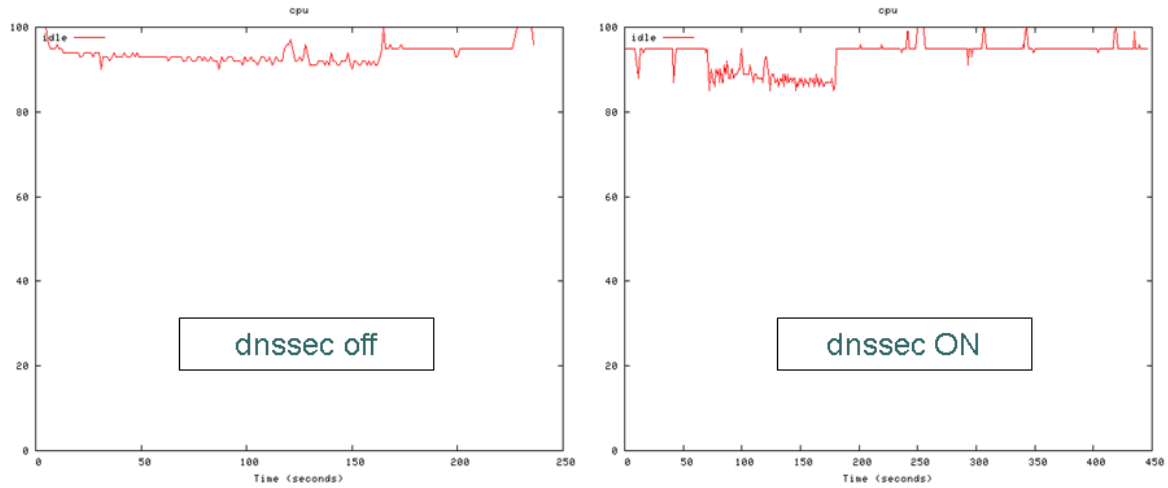
- テスト機に dnsperf/queryperf を導入しフルリゾルバに対して 負荷をかけ、処理状況をモニタ。
- サンプルの DNS クエリ情報を入手し試験に適したデータへ加工
- 試験に利用したデータは 10 万レコード(すべてが uniq ではない)
- パフォーマンス計測は vmstat および top を利用

<結果>

・DNSSEC 対応の DNS 要求を処理することでフルリゾルバに負荷上昇およびメモリ利用の増大が見られた。

■ 事例 3 実験結果詳細

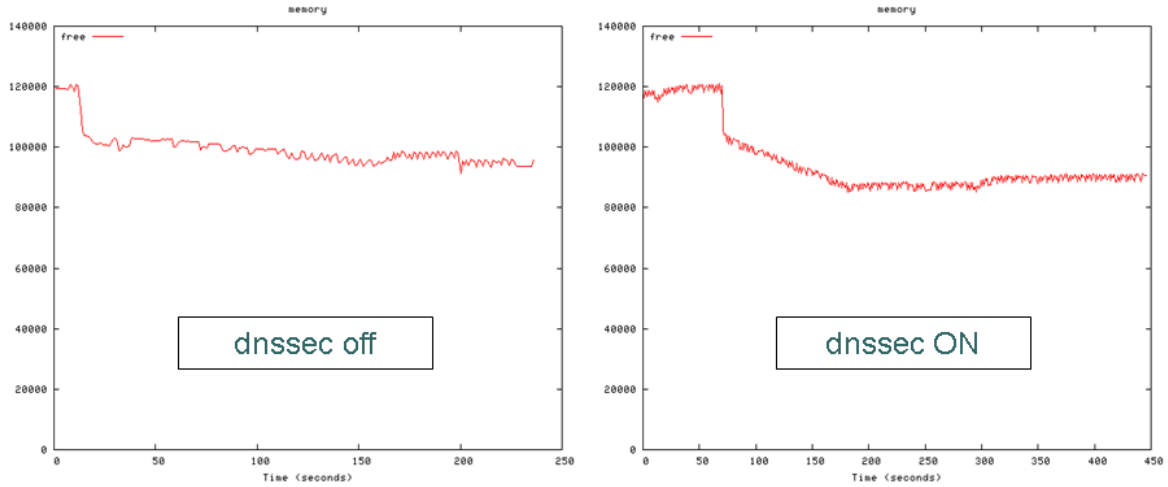
●dnssec On/Off での CPU 値の比較



DNSSEC off 時と比べ dnssec ON 状態だと CPU 負荷の上昇が確認できる。

(上位 NW の帯域制限等により、DNS 処理数が低下し、CPU 性能をすべて使用しきれていない)

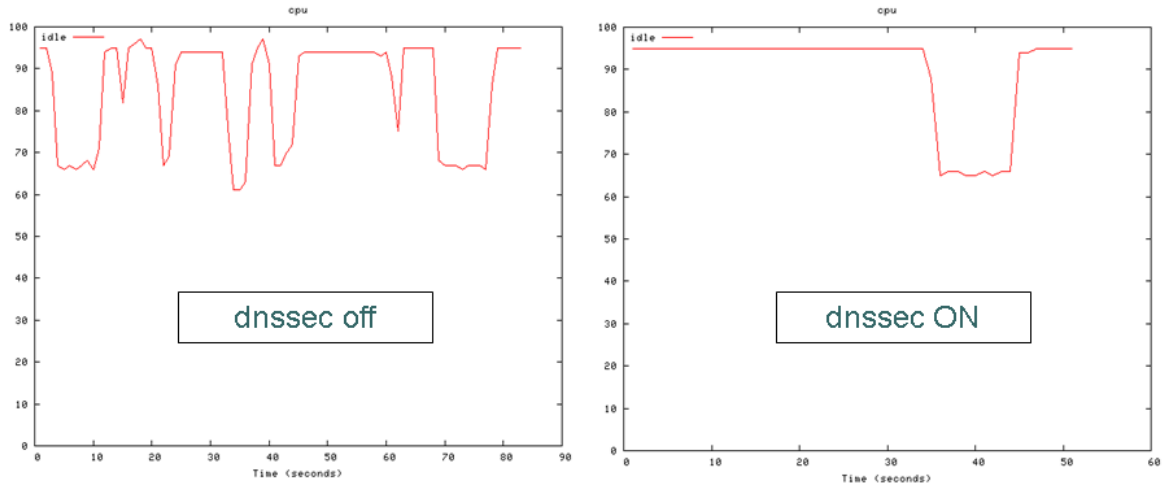
●dnssec On/Off でのメモリ値の比較



Off 時と比較して On 時のメモリ消費量は多いものの、一見して大きな差異はあらわれなかった。

(試験で利用した uniq クエリ数が少量の為にデータ差異が現れなかった可能性有り。

●フルキャッシュ時での CPU 比較



100%キャッシュ Hit 状態での CPU 負荷は dnssec の On/Off にかかわらずほぼ同じ値を示す。一度キャッシュした情報に関しては署名検証による影響は少ない(またはない)と思われる。

■ 事例 3 得られた知見

試験環境における性能比較については 試験環境またはネットワークの構成の制限により、大きな差異は見受けられなかった。

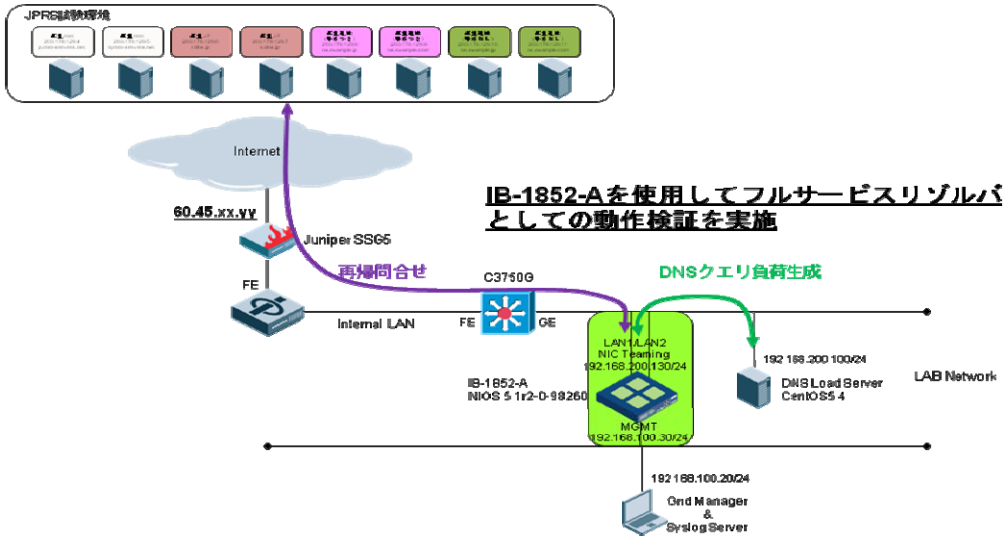
ただし、今回の実験でも DNSSEC を有効にすることによる負荷上昇は少なからず確認できる。DNSSEC の利用率によりフルリゾルバに対する負荷は変化することから、サービスを提供するフルリゾルバに対しては以下の状況を継続的にモニタし、システムの増強、増設を行う必要があると考える。

- メモリ使用量
- キャッシュヒット率
- サーバ CPU 使用量
- NW 帯域使用量
- コネクション数

さらに、キャッシュヒット率による性能差異が、DNSSEC Off 時と比べると顕著に表れるサーバの停止/起動(または キャッシュのクリア)に関しては、最繁時間を避ける等の考慮が必要と思われる。また、暖機運転の方法を確立しておく必要があると考える。

性能確認 事例 4

■ 事例 4 実験環境



DNS アプライアンス機器： Infoblox 1852-A Network Service Appliance

ソフトウェアバージョン： NIOS 5.1r2-0-98260 ※NIOS = Infoblox アプライアンスの内部 OS の呼称

■ 事例 4 実験結果概要

▼1 台の Linux 負荷生成サーバより IB-1852-A DNS キャッシュサーバに対し queryperf を使用して 100 ユニークドメインのテストクエリ（www.xxx.co.jp A）を 5 分間送信し、100% cache hit 時での DNSSEC validation 設定なしの状態と Validation 設定ありの場合のアプライアンスへの負荷の影響を確認した。

DNS 技術実験環境仮想ツリーの RSA 2024bit の試験環境を使用し、IPv4 アドレスのみ試験を実施した。

※DNSSEC 性能確認手順書 ver.1.2 に沿った検証項目は未実施です。

▼実験結果

本実験でのキャッシュサーバへの性能影響度合いとしては、DNSSEC validation 設定なしの状態と Validation 設定ありを比較した場合、Validation 設定ありの状態で約 13%の性能低下が確認できた。

DNS クエリ応答の RRSIG レコードのメッセージサイズ増加分が性能への影響を与えていることが確認できた。

■ 事例 4 実験結果詳細

▼IB-1852-A DNSSEC Validation 設定なし 100% Cache hit rate

queryperf　-D オプションなし

1 回目　　141238.4 qps　　アプライアンス平均 CPU 負荷　81%

2 回目　　142645.4 qps　　アプライアンス平均 CPU 負荷　84%

3 回目　　142131.4 qps　　アプライアンス平均 CPU 負荷　83%

4 回目　　141813.0 qps　　アプライアンス平均 CPU 負荷　82%

5 回目　　141439.3 qps　　アプライアンス平均 CPU 負荷　82%

DNSSEC Validation 設定なし dig 応答例

```
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> @192.168.200.130 www.xxxxx.co.jp A
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10029
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.xxxxx.co.jp.                IN      A

;; ANSWER SECTION:
www.xxxxx.co.jp.         861     IN      A       192.0.2.1

;; Query time: 0 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 24 20:44:34 2010
;; MSG SIZE  rcvd: 49
```

▼IB-1852-A DNSSEC Validation 設定あり　100% Cache hit rate

queryperf　-D オプションあり

1 回目　　123276.8 qps　　アプライアンス平均 CPU 負荷　83%

2 回目　　123065.5 qps　　アプライアンス平均 CPU 負荷　82%

3 回目　　123418.6 qps　　アプライアンス平均 CPU 負荷　84%

4 回目　　122981.4 qps　　アプライアンス平均 CPU 負荷　81%

5 回目　　123616.6 qps　　アプライアンス平均 CPU 負荷　84%

DNSSEC Validation 設定なし dig 応答例

```
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> +dnssec @192.168.200.130
www.xxxxx.co.jp A
; (1 server found)
```

```
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25119
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.xxxxx.co.jp.                IN      A

;; ANSWER SECTION:
www.xxxxx.co.jp.         666     IN      A       192.0.2.1
www.xxxxx.co.jp.         666     IN      RRSIG   A 8 4 900 20101225225717 20091225215717
24018 xxxxx.co.jp. GPTQObu3iCAksBwl5qAo+epHdEulfnA8dYW6MWGWLptfwMpZ/nJaYnur
GKc2MQh6zD5Q8RFFpdZrXWOWrqW9W8ffry5mmrdaEQxhSibmsoshw3GA
ymaM/J9F1UAfNQFPKLLHCGJUtdMbMxD5LtxaSBwRlO7rZFyGKPYeXgs2 HHs=

;; Query time: 0 msec
;; SERVER: 192.168.200.130#53(192.168.200.130)
;; WHEN: Tue Aug 24 20:41:58 2010
;; MSG SIZE  rcvd: 231
```

(※参考：テストで使用したシェルスクリプト)

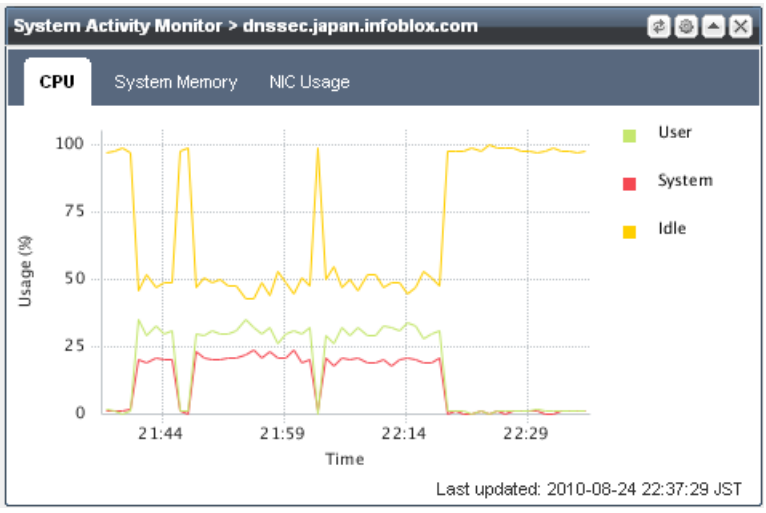
```
#!/bin/sh
SECS=300
INPUT=cached_test.data
SERVER=192.168.200.130
NUM=60
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out1 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out2 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out3 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out4 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out5 2>&1 &
./queryperf -s $SERVER -d $INPUT -l $SECS -q $NUM -D > out6 2>&1 &
wait
grep 'Queries per' out? | awk 'BEGIN { sum=0;}{ sum += $5;} END {printf("Total:
%.1f qps¥n", sum);}'
```

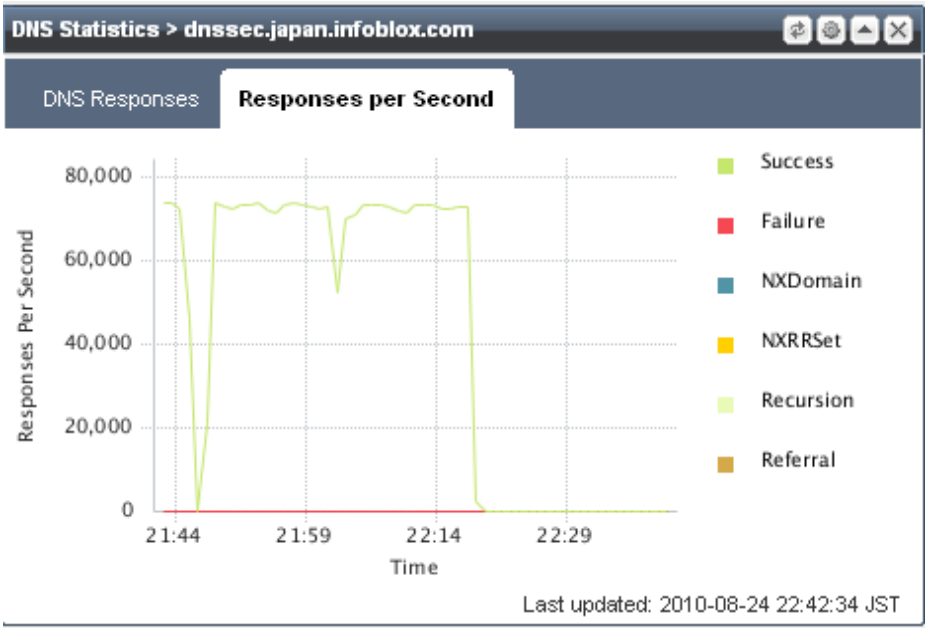
■ 事例 4 得られた知見

本実験では 100% cache hit の状態で DNSSEC Validation 設定あり・なしの条件でのみ計測を実施した結果となりますが、実環境への導入においては再帰問合せが発生する比率や DNSSEC Validation 設定時の平均応答サイズ等を考慮の上、キャッシュサーバへの性能影響を検討する必要があります。

（ご参考情報）

NIOS5.1r2 より Infoblox Grid 管理画面上で、CPU/Memory/NIC 使用率、DNS クエリ応答統計値をグラフで確認できるように機能拡張されております。





性能確認 事例 5

DNSSEC 化による権威 DNS サーバの負荷の変化

■ 事例 5 実験環境

DNS サーバ用のハードウェアを 2 種類用意した。1 台は比較的新しいもの、もう 1 台は比較的古いものである。

	CPU	OS
サーバ A	Xeon E5540 (2.53GHz) × 2	CentOS 5.5
サーバ B	Pentium-III 1.26GHz	FreeBSD 8.0

これらのサーバで BIND 9.7 系の named を動かし、LAN 接続の別サーバから dnsperf で負荷をかけ応答性能を計測し、DNSSEC 無し、DNSSEC 有りの場合の応答性能の変化を観測した。さらに DNSSEC 有りの場合については、NSEC 方式と NSEC3 方式を比較した。

DNSSEC 化による権威 DNS サーバの負荷の変化

計測に利用したデータ

- 計測対象のゾーンデータ
  実運用している小規模ドメイン名のゾーンデータ(総リソースレコード数 244)を、ほぼそのまま利用
- dnsperf で使うクエリデータ
  上記ゾーンの DNS サーバへのクエリログより生成したもの
  - 実際に発生しているクエリを利用しているが、DLV 環境を利用して DNSSEC 化しているため、DNSKEY の問い合わせなども含まれている
- DNSSEC パラメータ
  - 暗号化アルゴリズム RSASHA256
  - KSK の鍵長 2048bit
  - ZSK の鍵長 1024bit

■ 事例 5 実験結果

結果 1:　各方式の応答性能比較（単位 クエリ数/秒）

	方式	サーバ B (Pentium-III)		サーバ A (E5540)	
		存在	不在	存在	不在
DNSSEC 無	N/A	9345	8855	58423	58248
DNSSEC 有	NSEC	8352	7433	57279	56642
	NSEC3	7309	3364	57122	41437

存在：クエリログから存在するドメイン名のみ抽出

不在：存在から生成した不存在レコード

NSEC3 の Iterations:　5

計測中のサーバ A の CPU 使用率は 30～45%程度であった。queryperf を起動したサーバは、サーバ A と同スペックのものであるが、dnsperf がシングルスレッドのため充分な負荷発生させることが出来なかった可能性がある。したがってサーバ A の最大能力は更に高いと考えられる。サーバ B はいずれの計測においても CPU 使用率 100%となり、充分な負荷がかかっていた。

結果 2: 各方式の平均 DNS 応答サイズ

	方式	通常	存在	不在
DNSSEC 無	N/A	115	115	112
DNSSEC 有	NSEC	602	598	648
	NSEC3	637	604	884

通常：　クエリログをほぼそのまま適用(不在率 約 8%)

存在：　クエリログから存在するドメイン名のみ抽出（DNSKEY を含む）

不在：　存在から生成した不存在レコード

参考までに、DNS 問合せサイズは平均 45 バイトであった

■ 事例 5 得られた知見

DNSSEC 化により、権威 DNS サーバの応答性能はある程度低下する。この低下は、存在する名前の応答で 10～20%程度となる。特に NSEC3 の不在応答は、サーバによっては 50%以上の処理能力の低下を招くことがある。

DNSSEC 化により、権威 DNS サーバからの DNS 応答パケットは 5～8 倍程度に増加する。

性能確認 事例 6

NSEC3 方式の Iterations に対する応答性能の変化

DNSSEC 化する場合に NSEC3 方式を利用すると、Iterations の回数に応じてサーバの負荷が高まることが知られている、この変化を調査した。測定環境は前述の通りであるが、ゾーンデータを作成する際に Iterations の回数を 0～100 まで順に増加させたものを用意し、named に設定して queryperf コマンドでの応答性能を計測することを繰り返した。

■ 事例 6 実験環境

実験環境については、性能確認 事例 5 と同じである。

■ 事例 6 実験結果

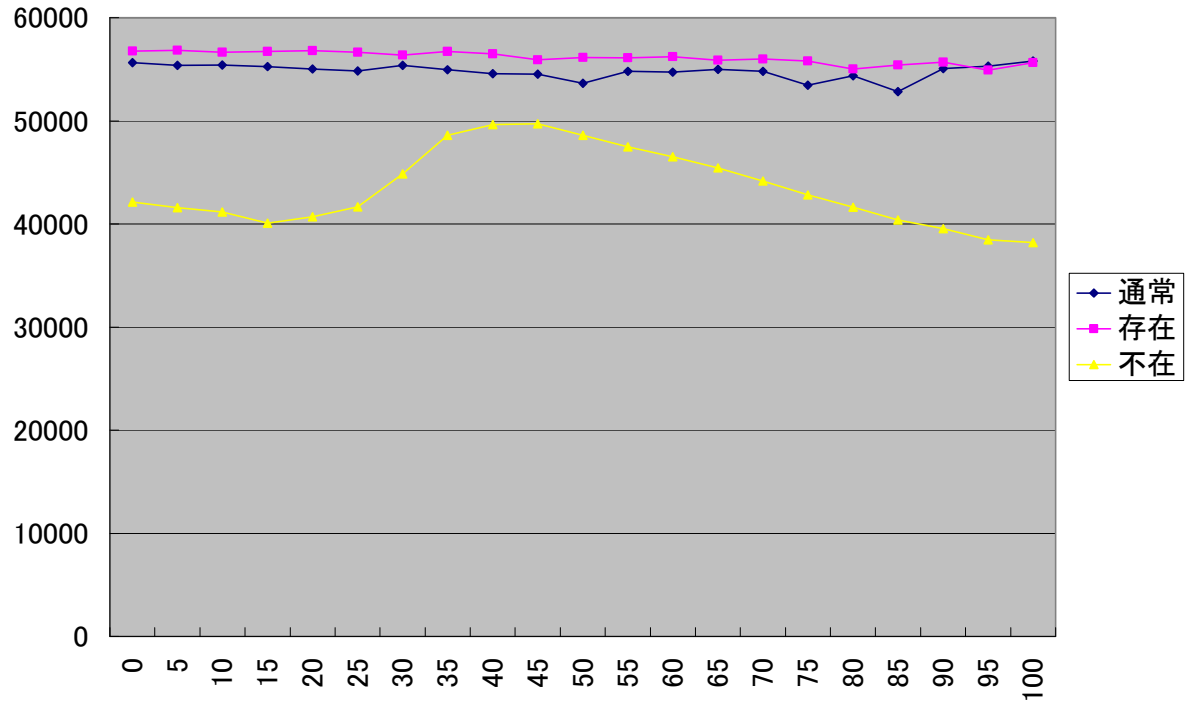
以下のグラフにおいて、通常、存在、不存在の意味は次の通りである。

通常：クエリログをほぼそのまま適用(不在率 約 8%)

存在：クエリログから存在するドメイン名のみを利用（DNSKEY を含む）

不在：存在から生成した不存在レコードのクエリ

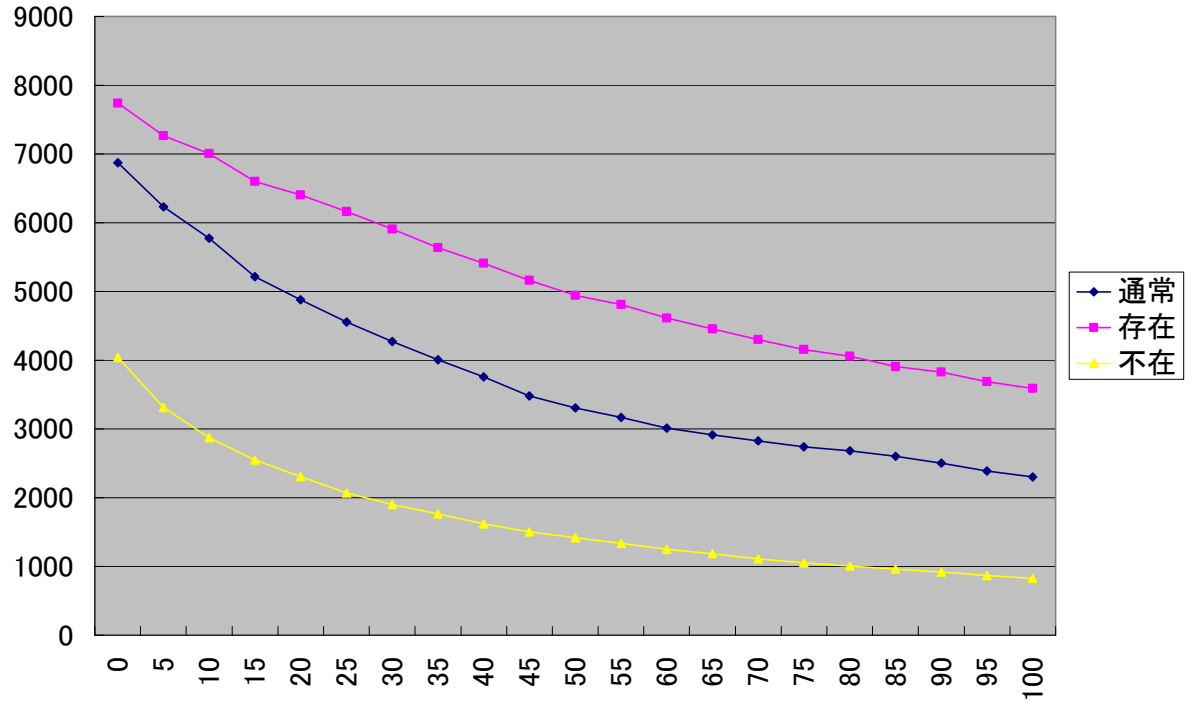
Iterations と応答性能の変化 サーバ A



x 軸：Iterations　y 軸:応答性能(qps)

この計測中、サーバ A における named の CPU 占有率は、最大で約 90% (Iteration 100 の不在応答時)となった。また Iterations の変化に対する不在応答の性能変化が不自然であるが、複数回計測しても同様の結果となったため、CPU の特性等、何らかの影響によるものと考えられる。

Iterations と応答性能の変化サーバ B



X 軸：Iterations　Y 軸:応答性能(qps)

サーバ B (Pentium-III)での存在応答の性能が、Iterations 増加に伴って悪化していることが伺える。NSEC3 においては、存在応答でもハッシュの計算を行う必要があるため、その影響と考えられる。

■ 事例 6 得られた知見

NSEC3 方式において Iterations を極端に大きな数字にするのは、応答性能に悪影響があるため、望ましくない。10 程度であれば実用上問題無いと言える。