技術検証結果の共有
JPRSにおける技術検証活動報告

2010年11月25日

DNS DAY @ IW2010

米谷嘉朗 <yoshiro.yoneya@jprs.co.jp>

Copyright © 2010 株式会社日本レジストリサービス

はじめに

- 本日紹介する技術検証の結果は、検証環境下における個別の事例であり、実環境下の全ての状況に共通するものではありません
- 自身の環境を検討する際の参考にとどめてください

Copyright © 2010 株式会社日本レジストリサービス

もくじ

- 技術検証の概要
- DNSサーバ・NW接続機器の検証結果
- レジストラ移転の検証結果

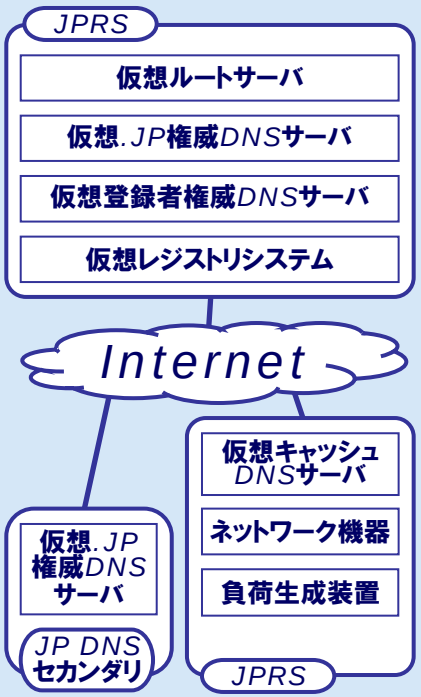
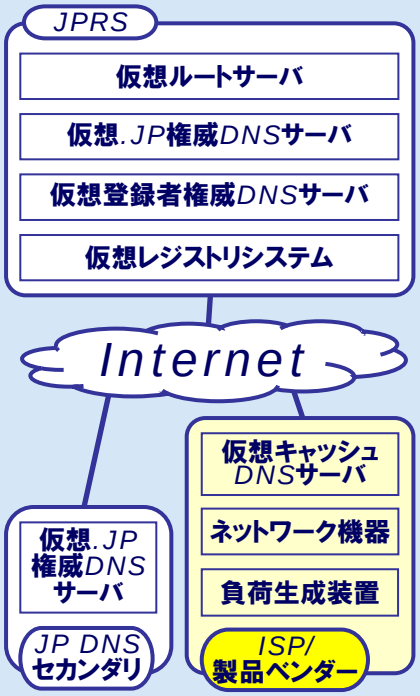
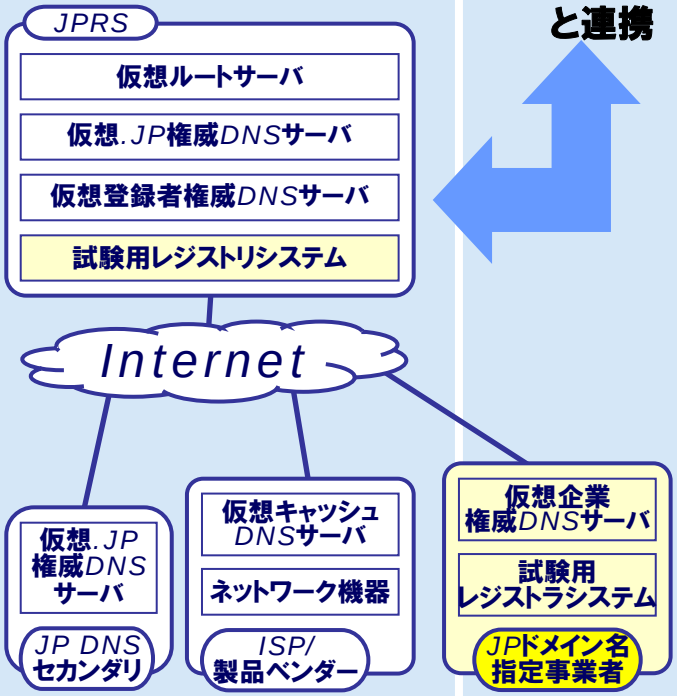
Copyright © 2010 株式会社日本レジストリサービス

技術検証の概要

Copyright © 2010 株式会社日本レジストリサービス

JPにおける取り組み【DNSSEC技術検証】

2010年11月現在

	ステップ1/ステップ2	ステップ3/ステップ4	ステップ5	ステップ6
概要	•JPRS社内に実験環境の構築 •権威DNSサーバ、キャッシュDNSサーバの機能・性能測定 •インターネットを介した仮想JP DNSセカンダリとのゾーン転送確認	•インターネットを介したISPの仮想キャッシュDNSサーバと接続 •ネットワーク機器等の製品ベンダーと協力し、機器のDNSSEC対応状況を確認	•試験用レジストリシステムの公開 •JPドメイン名の指定事業者の試験用レジストラシステムと接続 •JPドメイン名登録申請の動作確認	•DNSSECジャパンの成果に基づいた追加検証の実施 •DNSSECジャパンへ検証結果フィードバック
参加者	JPRS, JP DNSセカンダリ	JPRS, JP DNSセカンダリ, ISP, ネットワーク機器等の製品ベンダー	JPRS, JP DNSセカンダリ, ISP, ネットワーク機器等の製品ベンダー, JPドメイン名の指定事業者	DNSSECジャパン (http://dnssec.jp/) と連携
構成				

Copyright © 2010 株式会社日本レジストリサービス

ステップ1～5までの状況の説明(1/2)

- ステップ1
  - ローカルに実験を行い、DNSSEC機能確認手順書(*1)およびDNSSEC性能確認手順書(*2)を作成し、ステップ3・4の準備を実施

(*1) キャッシュDNSサーバおよび権威DNSサーバで、正しくDNSSECサービスを提供できるようにるために必要な各種動作を確認するための手順書。想定されるトラブルと、トラブルシュートためのシナリオという形式で確認手順を示している

(*2) キャッシュDNSサーバへの負荷および権威DNSサーバへのトラフィック変化を把握するための器構成と方式を示した手順書

- ステップ2
  - ゾーン転送の実験を行い、BINDの不具合を検出、ISCに報告してBIND 9.7.1で修正を反映

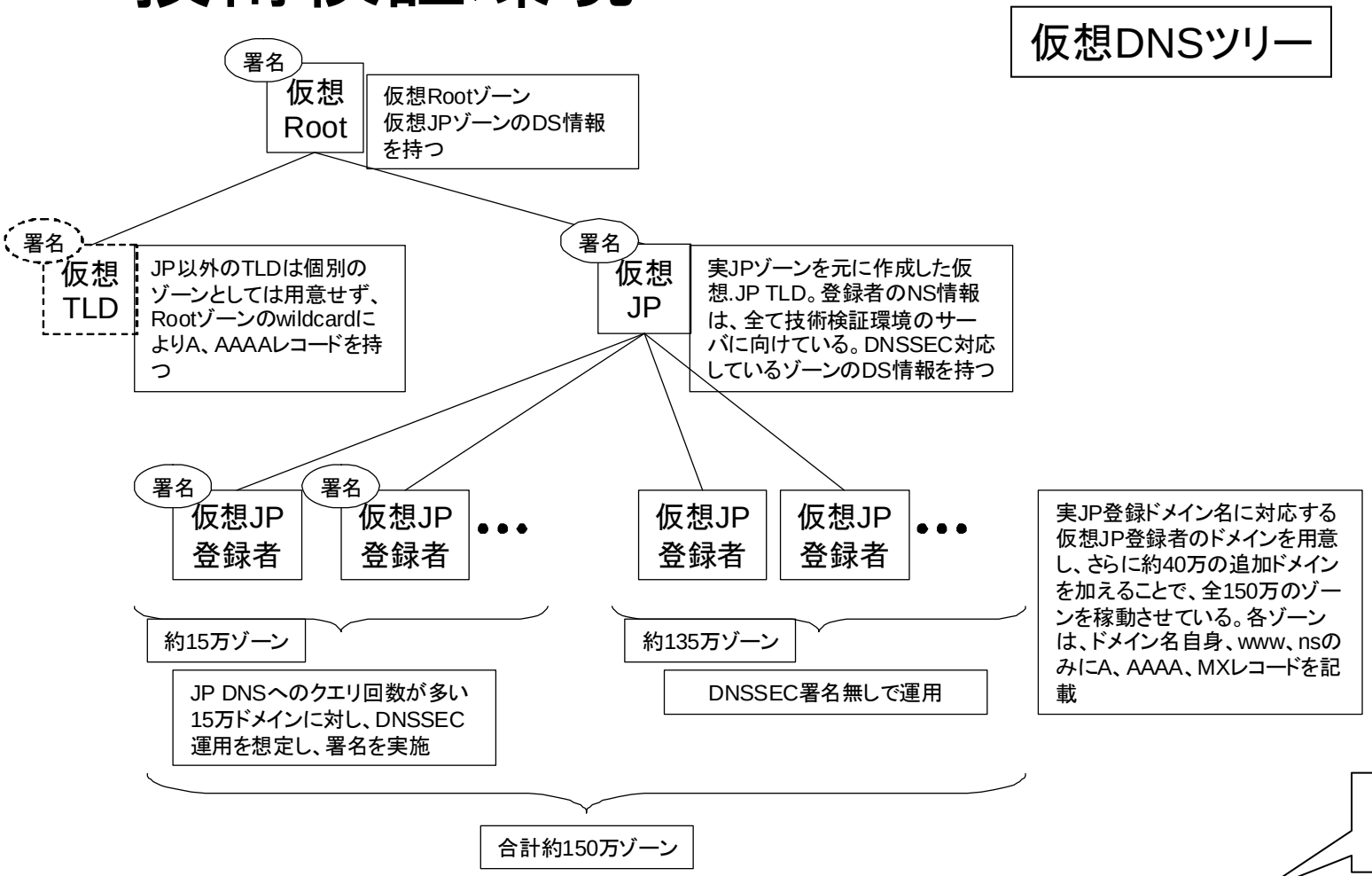
Copyright © 2010 株式会社日本レジストリサービス

ステップ1～5までの状況の説明(2/2)

- ステップ3・4
  - 数社のISPやハードベンダーと共同でキャッシュサーバおよびNW接続機器の挙動を確認、レポートを作成
  - 成果の一部はJANOG26等で紹介、レポートはJPRS Webで公開
- ステップ5
  - 数社の指定事業者と共同でレジストラI/Fの挙動やレジストラ移転の手順を確認、レポートを作成中
  - レポートはJPRS Webで公開予定

Copyright © 2010 株式会社日本レジストリサービス

技術検証環境



Copyright © 2010 株式会社日本レジストリサービス

DNSサーバ(キャッシュ・権威)・NW接続機器の検証結果

Copyright © 2010 株式会社日本レジストリサービス

検証方法

- 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、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
- 原則、以下2つの手順書にしたがう
  - DNSSEC機能確認手順書
    http://jprs.jp/dnssec/doc/DNSSEC-func-co-proc-v1.2.pdf
  - DNSSEC性能確認手順書
    http://jprs.jp/dnssec/doc/DNSSEC-perf-co-proc-v1.2.pdf

Copyright © 2010 株式会社日本レジストリサービス

機能確認事例1

- 対象
  - キャッシュサーバ
  - 権威サーバ
- 結果概要
  - キャッシュサーバは特に問題なし
- 知見
  - 権威サーバは、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倍になった
  - 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

Copyright © 2010 株式会社日本レジストリサービス

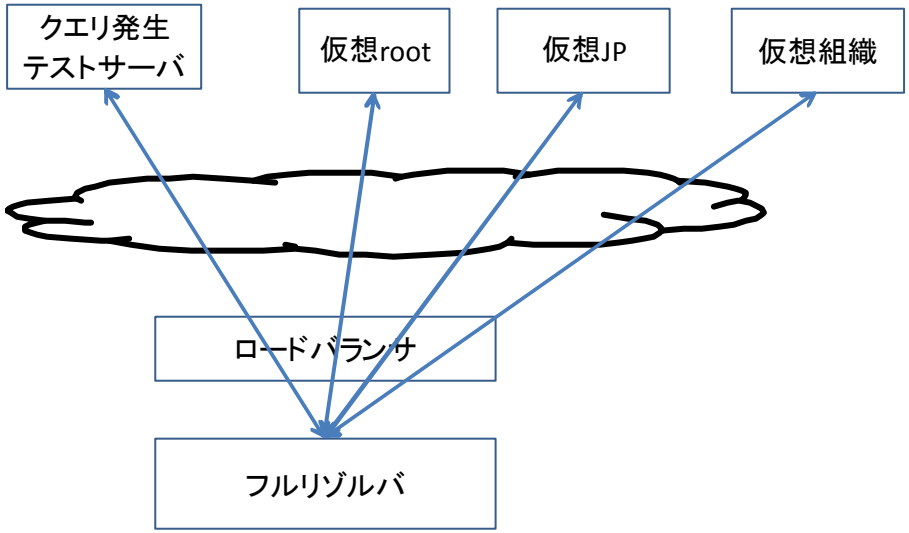
機能確認事例2

- 対象
  - キャッシュサーバ
- 結果概要
  - DNSSEC署名無→有でリソース消費量が変化した
    - 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
- 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

Copyright © 2010 株式会社日本レジストリサービス

機能確認事例3

- 対象
  - キャッシュサーバ
  - ロードバランサ
- 結果概要
  - 特に問題なし
- 知見
  - DNSSEC導入における機能的な問題はない



Copyright © 2010 株式会社日本レジストリサービス

機能確認事例4

- 対象
  - キャッシュサーバ
  - 権威サーバ
- 結果概要
  - 特に問題なし
- 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

Copyright © 2010 株式会社日本レジストリサービス

機能確認事例5

- 対象
  - DNSアプライアンス
- 結果概要
  - 特に問題なし
  - 未サポートの機能確認は未実施
- 知見
  - RSA/SHA-2に対応していないと検証に失敗する
    (ルートゾーン、JPゾーンはRSA/SHA-2で署名)
  - RSA/SHA-2対応版の導入を推奨する

Copyright © 2010 株式会社日本レジストリサービス

機能確認事例6

- 対象
  - ルータ
- 結果概要
  - 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、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
- 知見
  - 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

Copyright © 2010 株式会社日本レジストリサービス

機能確認事例7

- 対象
  - ルータ
- 結果概要
  - DNSSEC機能確認手順書の一部および[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機能の検証を実施
- 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
  - 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

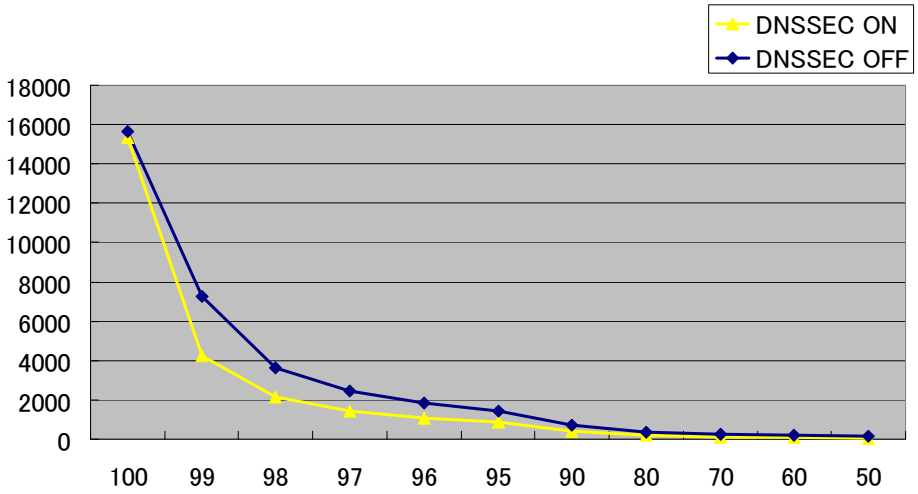
Copyright © 2010 株式会社日本レジストリサービス

性能確認事例1

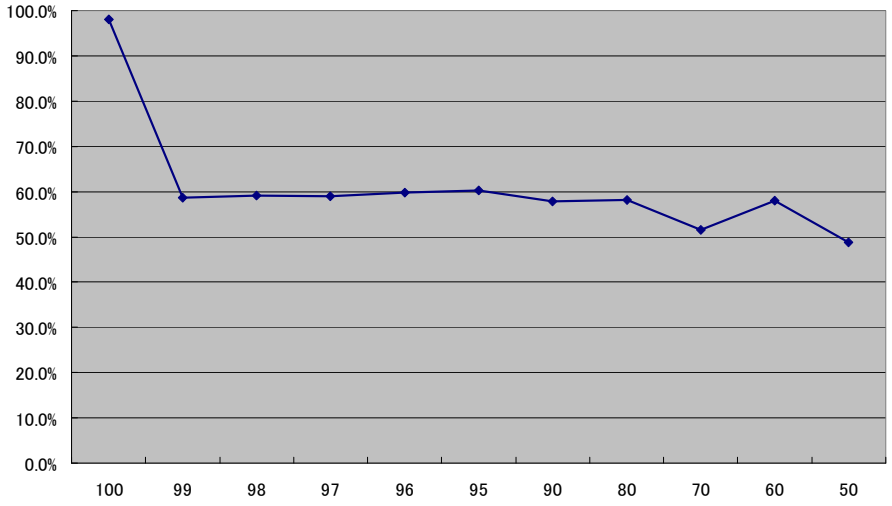
- 対象
  - キャッシュサーバ
- 結果概要
  - DNSSECを有効にすることにより、フルリゾルバでのCPU使用率上昇、メモリ使用量の増加、クエリ処理性能の低下を確認
- 知見
  - NSEC3使用、クエリがほぼNXDOMAINの状態ではメモリ使用量が8倍になった
  - DNSSEC ON時は、OFF時に比べクエリ処理能力が60%程度に低下した

Copyright © 2010 株式会社日本レジストリサービス

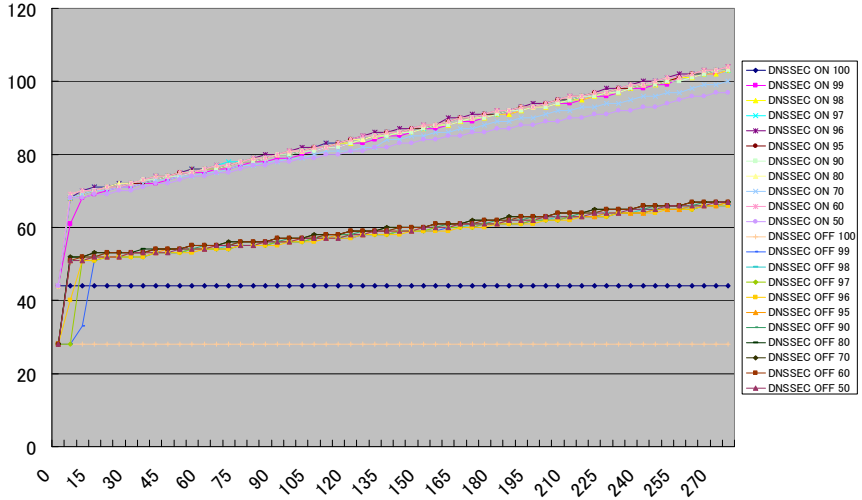
キャッシュヒット率ごとのqps



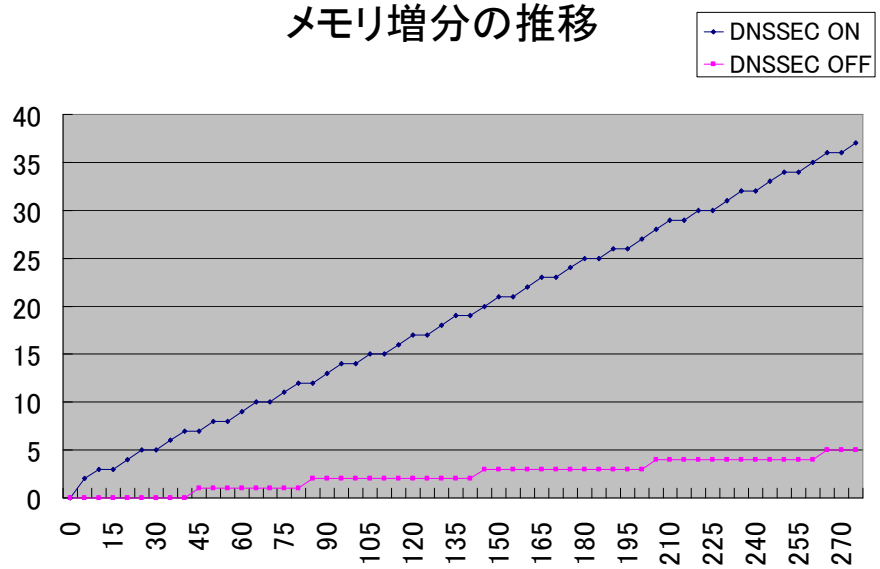
DNSSEC ON/OFF のqps比



メモリ使用量の推移



100qps、キャッシュヒット率80%時の メモリ増分の推移

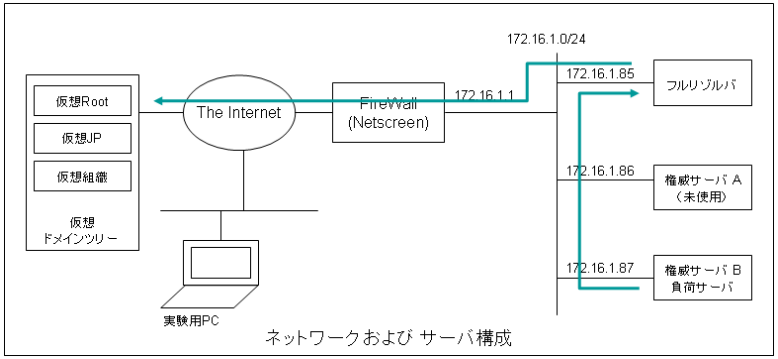


性能確認事例2

- 対象
  - キャッシュサーバ
- 結果概要
  - Validatorの各パターンによる挙動変化を計測
  - 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
- 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
  - 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

Copyright © 2010 株式会社日本レジストリサービス

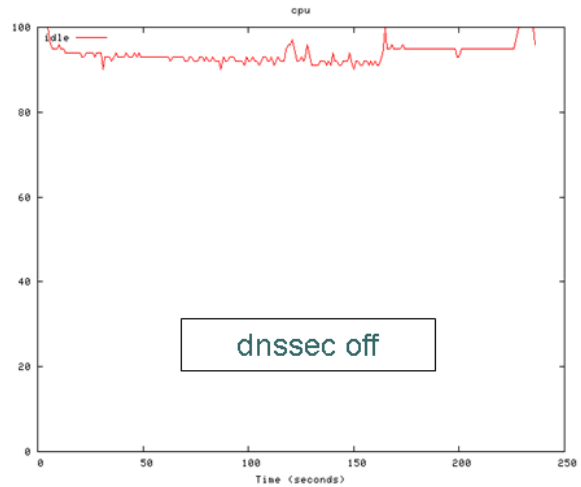
性能確認事例3

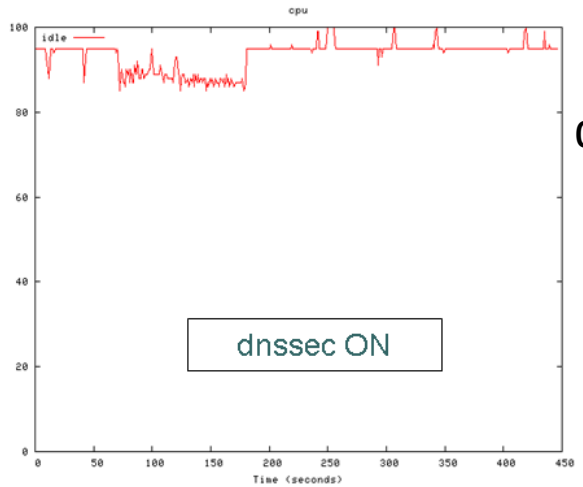


ネットワークおよび サーバ構成

- 対象
  - キャッシュサーバ
- 結果概要
  - 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
- 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、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た
  - 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
  - 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
    - 暖機運転の方法を確立しておく必要があると考える

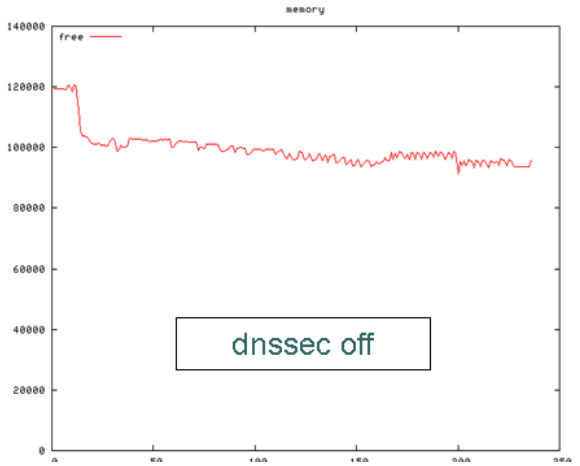
Copyright © 2010 株式会社日本レジストリサービス

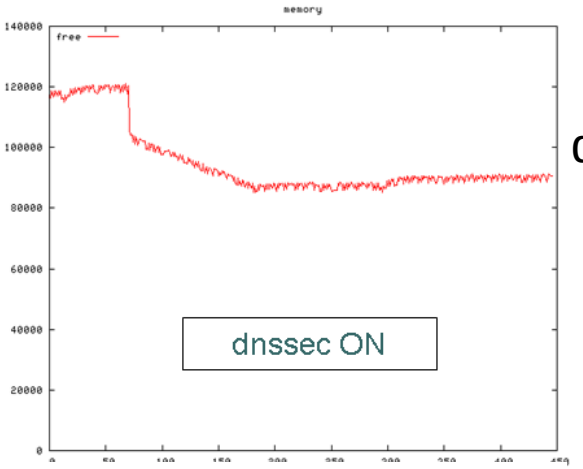




dnssec On/OffでのCPU値の比較

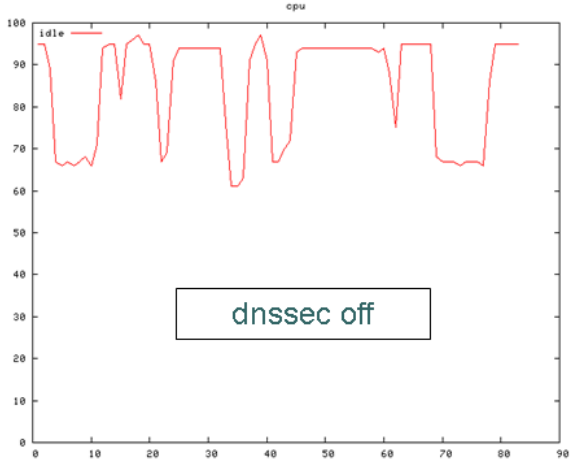
DNSSEC off時と比べ dnssec ON状態だとCPU負荷の上昇が確認できる
(上位NWの帯域制限等により、DNS処理数が低下し、CPU性能をすべて使用しきれていない)

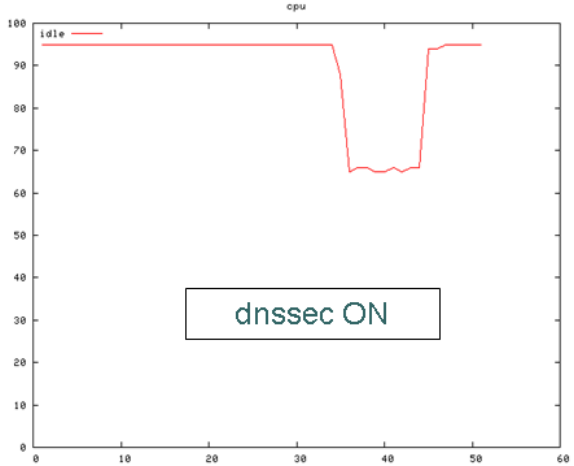




dnssec On/Offでのメモリ値の比較

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

性能確認事例4

- 対象
  - DNSアプライアンス
- 結果概要
  - 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
- 知見
  - 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る

Copyright © 2010 株式会社日本レジストリサービス

性能確認事例5

- 対象
  - 権威サーバ
- 結果概要
  - 性能の異なるサーバ(A:Xeon E5540、B：P-3)で応答性能の変化を観測
  - NSEC方式とNSEC3方式を比較
- 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

Copyright © 2010 株式会社日本レジストリサービス

応答性能(単位:クエリ数/秒)

	方式	サーバB(P-3)		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

(単位: qps)
NSEC3のIterationsは5

各不在証明方式毎の平均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

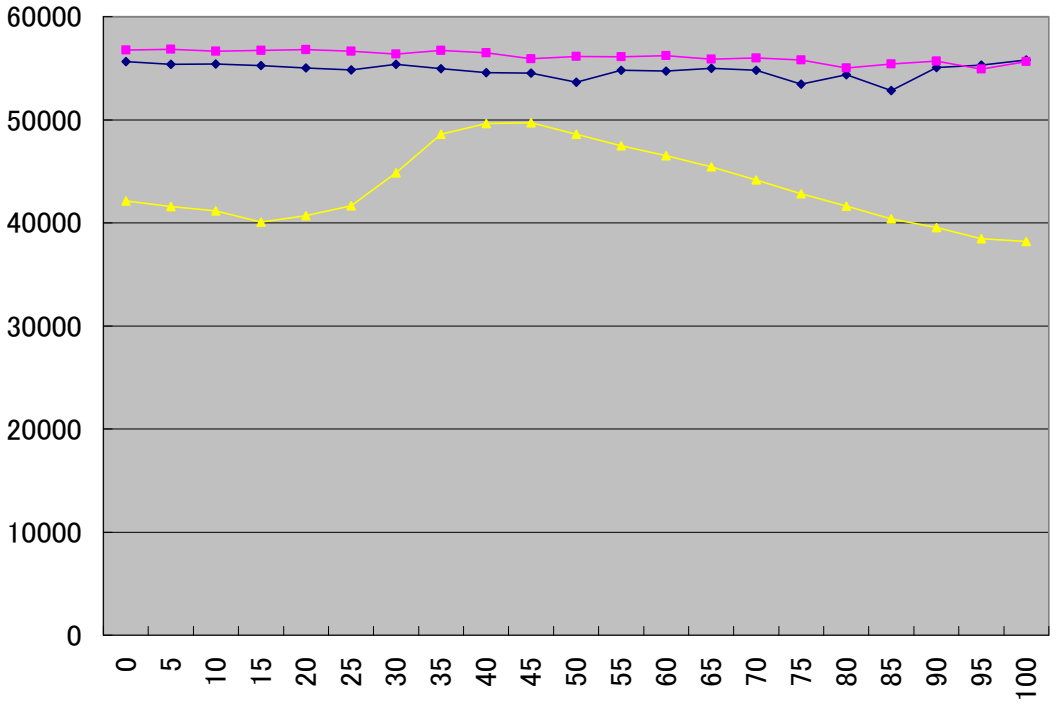
通常: クエリログをほぼそのまま適用(不在率 約8%)
存在: クエリログから存在するドメイン名のみ抽出
不在: 存在から生成した不存在レコード
※DNS問合せサイズは平均45バイト

Copyright © 2010 株式会社日本レジストリサービス

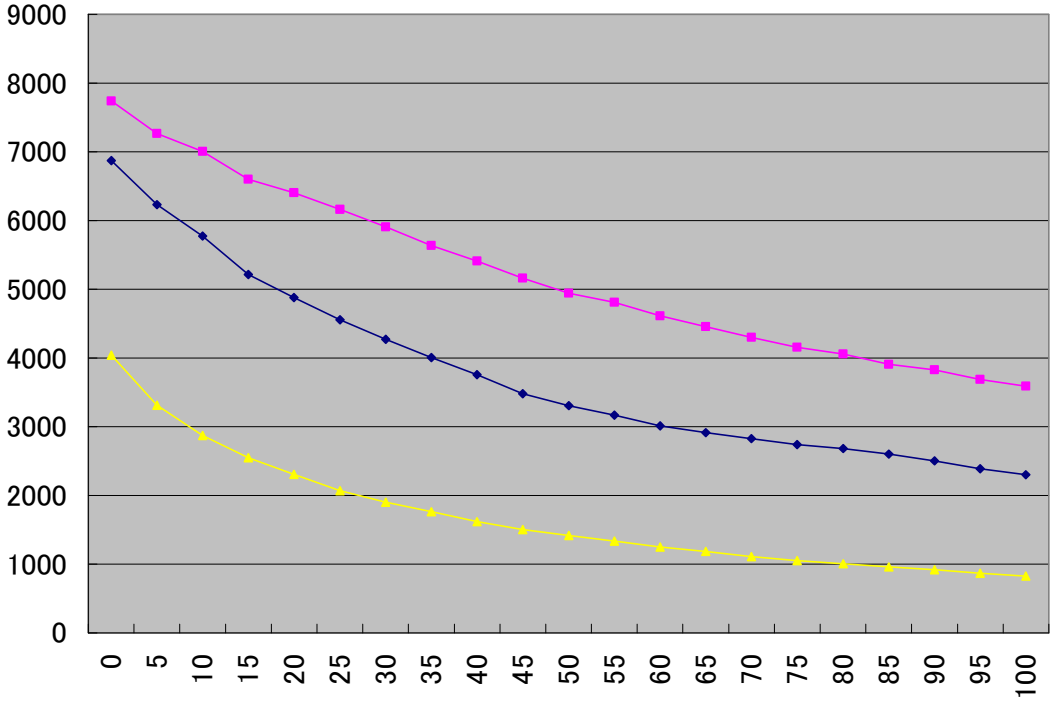
性能確認事例6

- 対象
  - 権威サーバ
- 結果概要
  - 性能の異なるサーバ(A:Xeon E5540、B：P-3)でNSEC3のIterations回数の違いによる応答性能の変化を観測
  - 低性能サーバではIterationsが増えると性能が低下
- 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

Copyright © 2010 株式会社日本レジストリサービス



Iterationsと応答性能の変化@サーバA



Iterationsと応答性能の変化@サーバB

実験実施社・報告書・発表等

- 実験実施社
  - インフォブロックス株式会社
  - NECアクセステクニカ株式会社
  - NECビッグローブ株式会社
  - NTTコミュニケーションズ株式会社
  - KDDI株式会社
  - ソネットエンタテインメント株式会社
  - 株式会社日本レジストリサービス
  - ヤマハ株式会社

- DNSSEC技術実験報告書 機能・性能確認編
  <http://jprs.jp/dnssec/doc/DNSSEC-testbed-report-fpv1.0.pdf>

- JANOG26「動かしてみましたDNSSEC 」
  <http://www.janog.gr.jp/meeting/janog26/program/dnssec.html>
- 2010 OARC Workshop 2 “An analysis of DNS queries sent from hosts to caching servers.”
  <https://www.dns-oarc.net/files/workshop-201010/oarc_iinou_zushi.pdf>
- IW2010 DNS DAY

Copyright © 2010 株式会社日本レジストリサービス

レジストラ移転の検証結果

Copyright © 2010 株式会社日本レジストリサービス

実験実施の背景

- ドメイン名登録者がドメイン名の取り次ぎ事業者(レジストラ)やDNSの預かり事業者(DNSプロバイダ)を移転(変更)することがある
- DNSSECに対応(署名)したドメイン名を移転する場合、DNSによる名前解決不能期間を生じさせないためには、従来の移転に比べて手順が複雑になる
- 代表的な移転手順を事例として確認し、業務化検討の基礎とする

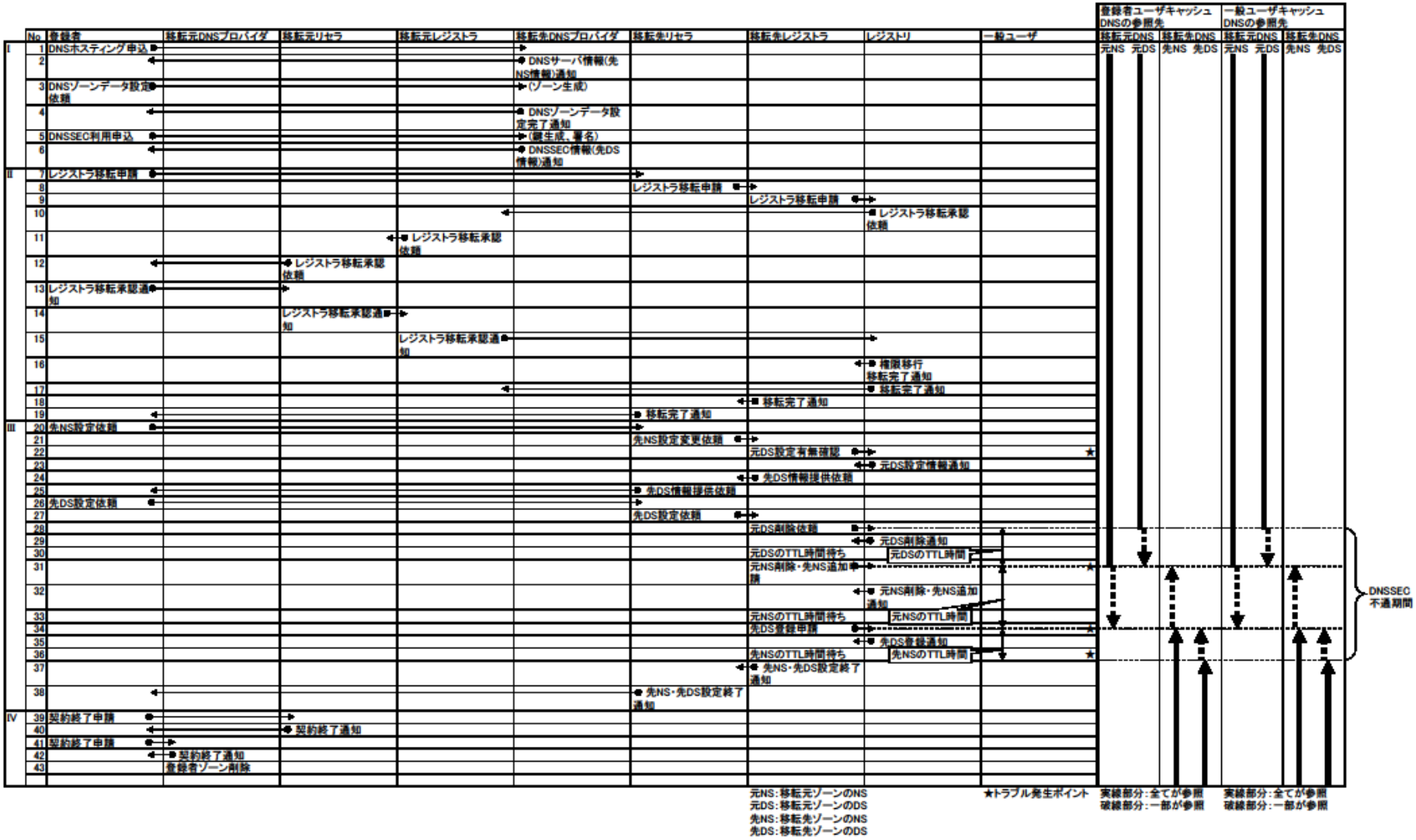
Copyright © 2010 株式会社日本レジストリサービス

実験概要

- 設定した前提条件
  - レジストラ移転と同時に、DNSプロバイダ移転が発生する
  - 移転元レジストラと移転先レジストラは相互にDNSSECの鍵情報は交換しない(レジストラ間の直接の情報交換は発生しない)
  - レジストラ移転・DNSプロバイダ移転の期間中もDNSの委任は継続する
  - レジストラはDNSプロバイダも兼ねる
- 実施手順の概要
  1. 移転先DNSプロバイダの準備を行う
  2. レジストラ移転を行う
  3. プロバイダ移転を行う
  4. 移転元DNSプロバイダおよび移転元レジストラの解約を行う
- 実験方法
  - 実験参加社が登場人物の役割を分担し、事前に想定したシナリオで一連の作業を実施

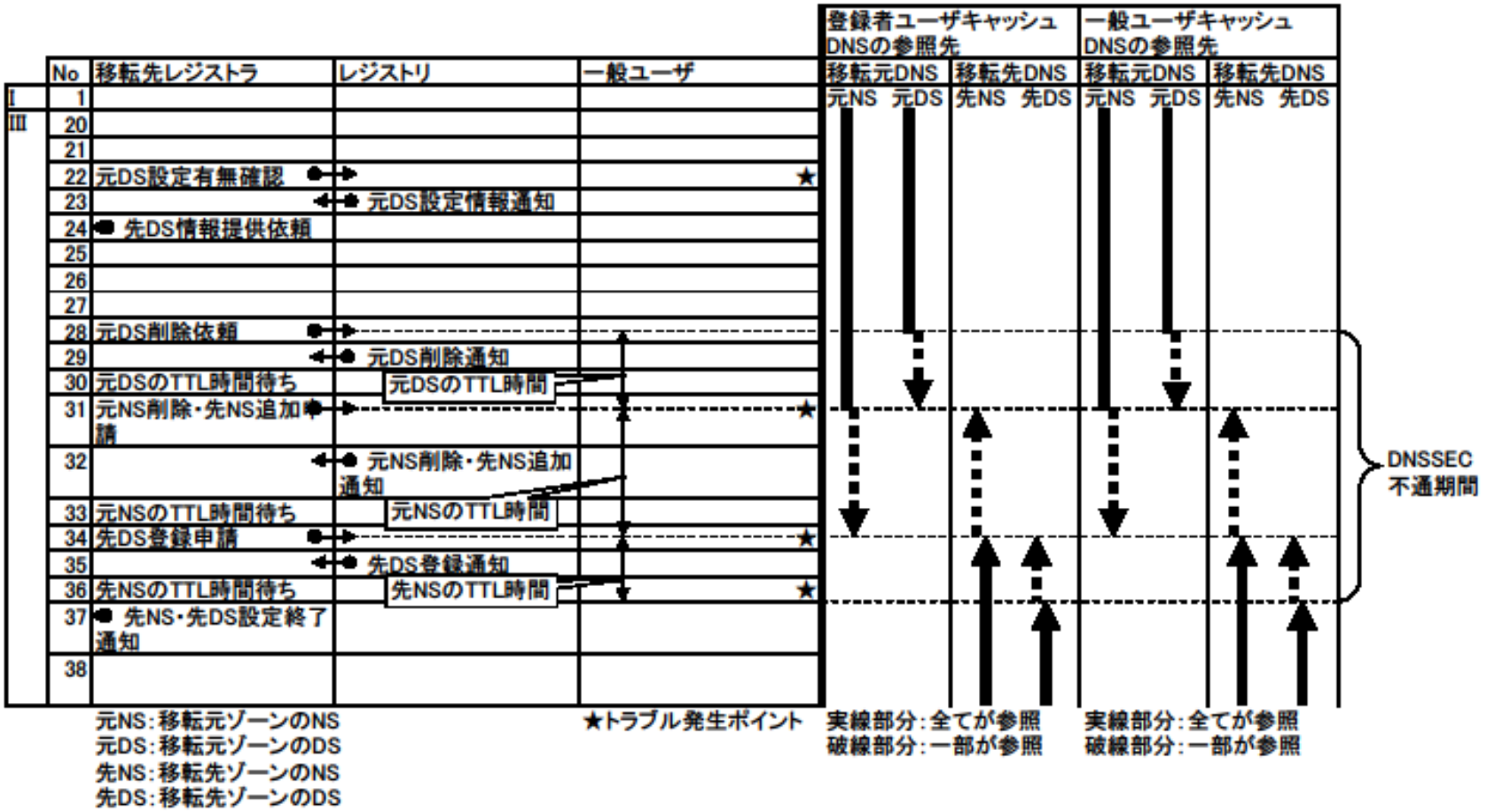
Copyright © 2010 株式会社日本レジストリサービス

移転フロー概要(全体)



Copyright © 2010 株式会社日本レジストリサービス

移転フロー概要(抜粋)



Copyright © 2010 株式会社日本レジストリサービス

知見

- 移転先レジストラは移転対象ドメイン名がDNSSECに対応しているか(署名されているか)を確認する必要がある
- 移転先レジストラはDSレコードのTTL値(レジストリが設定)およびNSレコードのTTL値(DNSプロバイダが設定)を把握して移転処理を実施する必要がある
  - DNSSECに関連してキャッシュサーバが保持するレコードはDS、NS以外にDNSKEYやネームサーバのA/AAAAもあり、トラブル発生時はそれらのTTLも考慮した対応が必要
  - ドメイン名登録者には、時間がかかることを説明することが必要
- 移転先レジストラが手順を誤ってトラブル(DNSの名前解決失敗)を生じさせた場合は、ISP(キャッシュDNSサーバ運用者)と連携して解決する必要がある
- 移転先レジストラは移転手順をどこまでエンドユーザにやってもらうか、またどの程度詳細に案内するかを判断しておかなければならない

Copyright © 2010 株式会社日本レジストリサービス

実験参加社・報告書・発表等

- 実験参加社
  - インターネットマルチフィード株式会社
  - NECビッグローブ株式会社
  - NTTコミュニケーションズ株式会社
  - 株式会社エヌ・ティ・ティ ピー・シー コミュニケーションズ
  - KDDI株式会社
  - さくらインターネット株式会社
  - ソフトバンクテレコム株式会社
  - 株式会社日本レジストリサービス
  - 株式会社ライブドア

- DNSSEC技術実験報告書 運用設計編
  - 2010年12月中旬にJPRS Web<http://jprs.jp/dnssec/doc/>で公開予定

- IW2010 DNS DAY

Copyright © 2010 株式会社日本レジストリサービス

Q and A

Copyright © 2010 株式会社日本レジストリサービス