ENUM トライアルジャパン
第 2 次報告書

2004 年 11 月

ENUM トライアルジャパン

目次

はじめに

ENUM は、電気通信番号をキーとして DNS を検索することにより、その電気通信番号に対応している、利用可能なひとつもしくは複数のアプリケーションを URI 形式で得る機構である。これにより、その URI で指定されたアプリケーション、たとえばその時点で利用可能な IP ネットワーク上の電話やメールなどへ接続が可能になる。

2002 年の 9 月に、社団法人日本ネットワークインフォメーションセンター(以下、JPNIC)が事務局となって設立した『ENUM 研究グループ』は、ENUM 技術そのものの検討や、ENUM の実現方式・運用方式、これに関連する技術的・制度的な課題の抽出などを行った。その後、ENUM を用いた通信サービス基盤技術の「実験」を推進するトライアルグループの需要が高まってきたことを受け、JPNIC、株式会社日本レジストリサービス(以下、JPRS)、WIDE プロジェクト(以下、WIDE) が発起人となり、2003 年 9 月 17 日に『ENUM トライアルジャパン(以下、ETJP)』が設立され、本格的なトライアルが開始されるに至った。

ETJP は、DNS による基盤サービスから通信アプリケーション、通信サービスまでを含めた基本機能と実用性の技術的検証、サービス化に向けた技術的課題の整理と検討を行う場としている。設立当初は 20 会員でという規模でスタートしたが、設立から 1 年が経過した 2004 年 11 月現在では、その数も 45 会員に増え、実験も進み、成果も出ている。

2004 年 5 月には、計画に基づく活動の前半を終えたとして、主にアプリケーションを中心とした実験の成果を第 1 次報告書としてまとめたが、本報告書では、それ以降、2004 年 11 月までの ETJP の活動を整理し、特にセキュリティや ENUM DNS の性能といったワーキンググループの活動報告を中心にまとめることとした。

今後の活動に向けて、関係者から様々な意見を頂戴できればありがたい。

2004 年 11 月　ENUM トライアルジャパン
会長　後藤　滋樹

1. 会員名簿

<団体>

株式会社アズジェント
株式会社アステック
株式会社アンネット
岩崎通信機株式会社
エヌ・ティ・ティ情報開発株式会社
NTT 番号情報株式会社
株式会社 NTTPC コミュニケーションズ
沖電気工業株式会社
グローバルメディアオンライン株式会社
KDDI 株式会社
株式会社サイネックス
株式会社ジェイ・エス・エス
シスコシステムズ株式会社
ソフトバンク BB 株式会社
株式会社ソフトフロント
ソリス株式会社
ディーシーエヌ株式会社
株式会社ディーネット
株式会社テリロジー
西日本電信電話株式会社
日本テレコム株式会社
日本電気株式会社
日本電信電話株式会社
社団法人日本ネットワークインフォメーションセンター
日本ベリサイン株式会社
日本マルチメディアサービス株式会社
株式会社日本レジストリサービス
パナソニック コミュニケーションズ株式会社
株式会社パワードコム
東日本電信電話株式会社
株式会社ピクト
株式会社日立製作所
VoIP 推進協議会
富士通株式会社
フュージョン・コミュニケーションズ株式会社
フリービット株式会社
松下電器産業株式会社
三菱商事株式会社
三菱電機情報ネットワーク株式会社
ヤマハ株式会社
株式会社 ライブドア
WIDE Project
早稲田大学理工学部後藤滋樹研究室

<個人>

伊藤　篤敬
福嶋　一

(全 45 会員・50 音順)

2. 活動の概要

2.1 全体会合

会員が、活動やその成果の発表、検討課題の議論、今後の方向性などの検討を行う場として、定例会議である『全体ミーティング』を 1～2 ヶ月に 1 度程度の頻度で開催した。表 1 に示すように、2004 年 5 月に第 1 次報告書の発行以来、設立総会を含め 5 回の全体ミーティングをもち、議論を行った。

表 1 全体ミーティングの開催状況

日	会合名	場所	出席会員数/全会員数	主な内容
2004.5.12	ETJP 第 1 次報告会	早稲田大学	30 会員/43 会員 (公開で行ったため、全 51 社 113 名が参加)	-ETJP の全体の活動報告 -ワーキンググループ活動報告 -JPRS、シスコシステム、日本テレコム、パナソニックコミュニケーションズのデモ -講演「VoIP 協議会と ENUM」
		http://etjp.jp/about/activity/20040512.html		
2004.7.28	第 5 回 ETJP 全体ミーティング	早稲田大学	24 会員/ 45 会員	-ワーキンググループ活動報告 -APEET、ITU-T SG2 報告 -講演「Update from SIP / ENUM Trial in Taiwan & IPOX Project」
		http://etjp.jp/about/activity/20040727.html		
2004.9.14	第 6 回 ETJP 全体ミーティング	早稲田大学	26 会員/ 45 会員	-ワーキンググループ活動報告 -IETF 報告、Apricot2005 について -アステックのデモ -今後の ETJP の活動について
		http://etjp.jp/about/activity/20040914.html		
2004.9.14	ETJP 第 2 回 総会	早稲田大学	32 会員(書面表決含む)/ 45 会員	-ETJP 設置期間延長承認の件
		http://etjp.jp/about/activity/20040914.html		

2.2 ETJP の外部への紹介活動

ETJP や ETJP 活動の紹介を国際会議や外部関連組織のミーティングで行ってきた。主なものは、表 2 の通りである。

表 2 ETJP の外部への紹介活動

日	主催	会合名	発表内容	特記事項
2004.5.21	APT/ITU	APT-ITU Joint Workshop on ENUM and IDN	ETJP の活動紹介	
2004.6.28	NetWorld+Interop 2004 Tokyo 実行委員会	NetWorld + Interop 2004 Tokyo	URI による識別と ENUM	

3. 活動内容詳細

3.1 Working Group における検討状況

3.1.1 Privacy and Security Working Group (PandS WG)

Privacy and Security Working Group の活動内容と、活動の成果として策定した二つの文書「ETJP 実験参加におけるプライバシーに関する注意喚起のためのメモ」、「ETJP システムにおけるセキュリティについて」について報告する。

3.1.1.1 活動内容報告

■設立経緯

ETJP 第 1 回全体ミーティング（2003 年 10 月 23 日）において、会員より、ETJP 参加メンバーにおけるセキュリティ対策について、最低限のものを共通ルールとして決めることが提案された。プライバシー・セキュリティ WG（Privacy and Security (PandS) WG）は、本提案を契機に、ETJP の各実験フェーズにおけるデータの取り扱いポリシーの検討及びガイドライン作成のため、ETJP 第 2 回全体ミーティング（2003 年 12 月 8 日）において ETJP 副会長の石田慶樹氏より設立が提案され、了承された。

■検討内容

PandS WG では、ETJP の実験フェーズ 2 および 3 への参加におけるデータの取り扱いポリシー、すなわち(1)ETJP 会員に適用されるプライバシーの考え方、及び、(2)ETJP の DNS 等のシステム全般に適用されるセキュリティの要件について検討を行った。検討は、メーリングリスト及び打ち合わせ開催等により進められた。

■成果

検討の結果、次の 2 文書を策定した。文書（案）は ETJP 第 5 回全体ミーティング（2004 年 7 月 27 日）および第 6 回全体ミーティング（2004 年 9 月 14 日）にて会員に提示、意見照会された。WG では、意見を反映後、本報告書の公開にあわせて策定された。

1. プライバシーの考え方・ポリシー

「ETJP 実験参加におけるプライバシーに関する注意喚起のためのメモ」
http://etjp.jp/about/wg/PandS-privacy.pdf

<<概要>>
ETJP に参加するにあたって、(1)その手段として DNS を使用すること及びその影響範囲、(2)その際に発生するプライバシー上のリスク、(3)ETJP において参加者が心掛けるべき事柄、などについて考慮点を整理したものである。

2. セキュリティ要件
「ETJP システムにおけるセキュリティについて」
http://etjp.jp/about/wg/PandS-security.pdf

<<概要>>
ETJP システムにおいて遵守すべきセキュリティポリシーについて、(1)ETJP が保有する情報の種類、(2)関連するユーザの種類、を整理した上で、ETJP の系全体としてのセキュリティ要件を段階的な重要度により分類し、これをシステム各部に対し適用したものである。また、このポリシーに照らし合わせて、現在構築されているシステムの評価を行っている。

上記 2 つの文書については、3.1.1.2 と 3.1.1.3 で、全文を紹介する。

■成果の位置づけ

両文書の内容は、本報告書の公開以降、ETJP の実験フェーズ 2、3 に参加する ETJP 会員に適用されることとする。（注：特に、セキュリティ要件については、ETJP 会員の設備に対して強制力を持つ内容もある）将来、実験の前提条件（例：ENUM 用トップレベルドメイン、実験用番号等）が変更される場合は、本内容をベースに内容の見直しについて検討することとする。

■参考：検討スケジュール

2003 / 12 /　25 ～ML における議論開始
　　検討内容・前提条件等を整理
2004 / 04 / 15　第 1 回 WG ミーティング
2004 / 04 / 30　第 2 回 WG ミーティング

2004 / 06 / 24　第 3 回 WG ミーティング
2004 / 07 / 21　第 4 回 WG ミーティング
　　プライバシーの考え方、セキュリティ要件（案）を検討、策定
2004 / 07 / 27　ETJP 第 5 回全体ミーティング
　　会員にプライバシー・セキュリティの文書（案）を提示、意見照会
2004 / 08 / 06　会員からの意見締め切り
2004 / 09 / 14　ETJP 第 6 回全体ミーティング
　　プライバシーの考え方を再提示、意見照会
2004 / 11 / 10　ETJP 報告書の公開
　　ETJP 実験におけるプライバシーの考え方、セキュリティ要件を
　　策定

3.1.1.2「ETJP 実験参加におけるプライバシーに関する注意喚起のためのメモ」(全文)

1. ETJP 実験に参加するにあたって

・DNS への登録の必要性
－ENUM を利用するアプリケーションはネームサーバに登録されたデータを検索し適切な動作を行います。
－ENUM を利用するにあたってエンドユーザのデータをネームサーバに登録する必要があります。
－エンドユーザのデータとはメイルアドレスや SIP アドレスでありプライバシー情報ともなりえるものです。

・DNS への登録による起こる作用
－ネームサーバに登録することによりインターネット全体に情報が公開されることになります。
－情報が公開されたことにより全世界からの本来の目的である ENUM によるアクセスが可能になります。
－しかし公開された情報は本来の利用目的以外にも利用される可能性が非常に高いことも想定されています。

2. DNS への登録による発生すると想定されるリスク

・DNS に登録されたデータの目的外取得による不正利用や利用妨害
－網羅的な探索による名簿やデータベース等の作成行為
ー適切な利用者への検索を妨害する行為(DoS)

－DNS の問い合わせや返答に対しての盗聴や偽造

・DNS に登録された情報を利用した迷惑な行為
－いたずら電話
－SPAM 電話
－ワンギリ
－勧誘電話

・DNS へのデータの不正な登録
－正当な登録の妨害やなりすまし

3. ETJP でのプライバシーの考え方

・ETJP で規定した方法により守れること
－DNS の問い合わせや更新を DNSSEC を利用することと、登録を SSL を利用して ID とパスワードを管理することにより、登録されたデータの完全性を保証するとともに、不正登録やなりすましを防止することが可能です。

・ETJP で規定した方法によっても守れないこと
－登録されたデータの不正利用および不当行為を防止することはできません。

4. ETJP でのプライバシーの懸念

・リスクを低減するために登録者が行うべきこと
－ENUM を利用するにあたっては先に述べたリスクから完全に逃れる方法は今のところありません。
－したがって ENUM を利用するにあたっては登録するデータは法人や団体としてのみのデータを登録し、個々人のデータを登録するにあたっては慎重に行う必要があります。
－このようなリスクが存在していることから、データを登録するにあたっては、登録する主体(個人・団体)においてリスクを認識した上での「オプトイン」に基づいたデータ登録を行う必要があります。

3.1.1.3 「ETJP システムにおけるセキュリティについて」(全文)

0. はじめに

・この文書の目的

－ETJP システムに関する現状を記述する

－ETJP システムについての

・セキュリティ的観点からの評価・要件整理を

・既存の ENUM モデルに照らし合わせることにより実施する

1. ETJP 申請情報の分類

・会員情報

－組織情報、活動への貢献内容、責任者情報、事務連絡先情報

・ETJP 番号情報

－+8100 配下の７桁以上１２桁以下の任意の番号

・DNS 資源情報（NS,NAPTR,DS）

－ETJP 番号に対し設定する DNS リソースレコード

－NS 登録は Tier1 DNS 機能、NAPTR 登録は Tier2 DNS1 機能

－NS 登録時には DS（DNSSEC 機能）登録を併せて行うことが可能

2. 関連するユーザの分類

・ETJP ENUM レジストリ

－Tier0 相当のネームサーバ運用を行う

－e164.jp をゾーンとして使用

－e164.arpa の委任を受けるまでの暫定運用

－運用実体は JPRS

・ETJP 事務局‥認証局相当

－ETJP において会員入会管理を行う

－会員の ID/パスワードを発行

・ETJP レジストリ‥Tier1＋2　レジストリ・レジストラ相当

－ETJP　レジストリシステム・DNS の運用・管理を行う

－会員に電話番号空間の割り振りを行う

－会員から NS 設定申請を受け、処理する

－会員から NS 設定申請を受け、処理する

－会員から NAPTR 設定申請を受け、処理する

・ETJP 会員‥Tier2 レジストリ・レジストラ＋レジストラント相当

－JPRS に対し番号空間取得の申請を行う
－ETJP 番号に対する NAPTR または NS レコードを登録する
－NS レコード登録時は、会員自身で Tier2 DNS を設定する

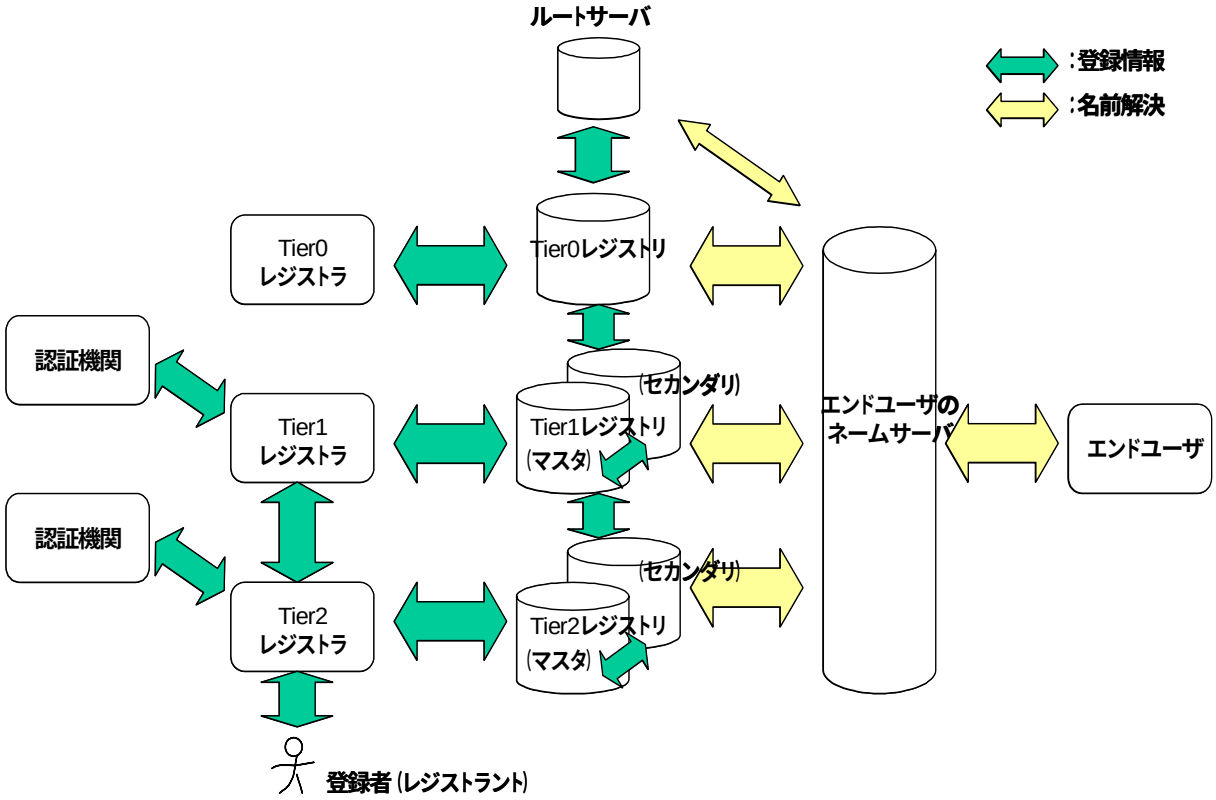
3. 用語について

・MUST　　要件を満たすためには実装・対応が必須
・SHOULD　　要件を満たすためには実装・対応されるべき
・RECOMMENDED　　要件を満たすためには実装・対応されるのが望ましい
・MAY　　要件を満たす上で実装が行われてもよい

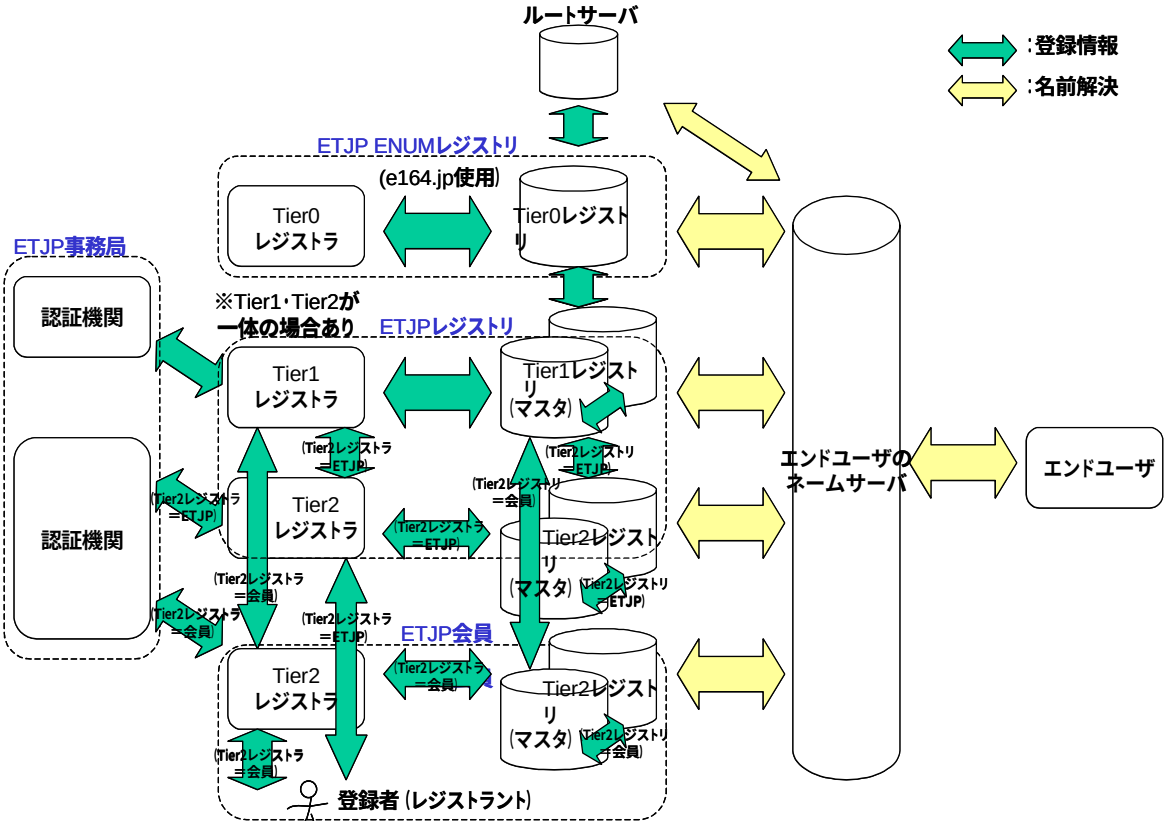
→上のものほど要求度合いが高くなる
→基本的には RFC2119 の定義に従う

4. ENUM における役割定義について

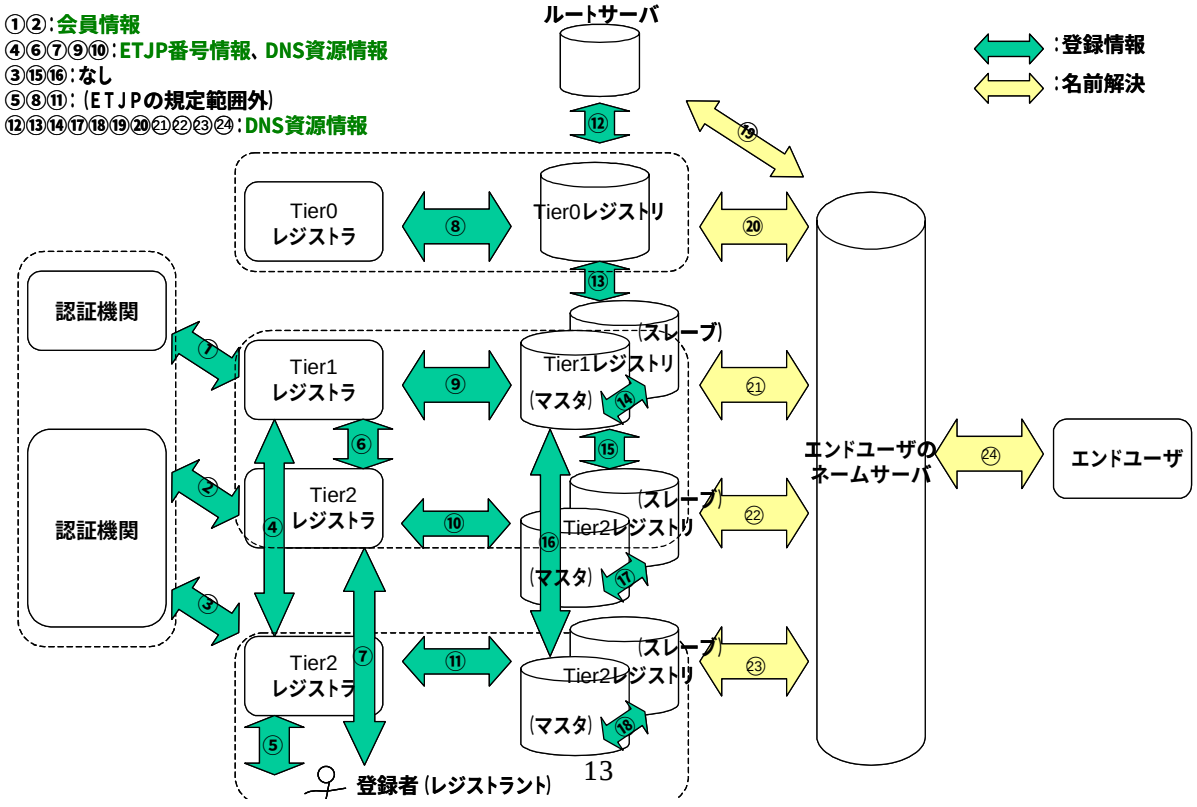
（参考:ENUM 研究G報告書　P64　米 ENUM フォーラム　ENUM Forum Specification for US implementation of ENUM　P13-14）



4-1　ETJP における役割定義について



5. ETJP の役割（間）において扱う情報について



6. ETJP の役割（間）に適用するセキュリティについて

①②④⑦：https (ID+PW)

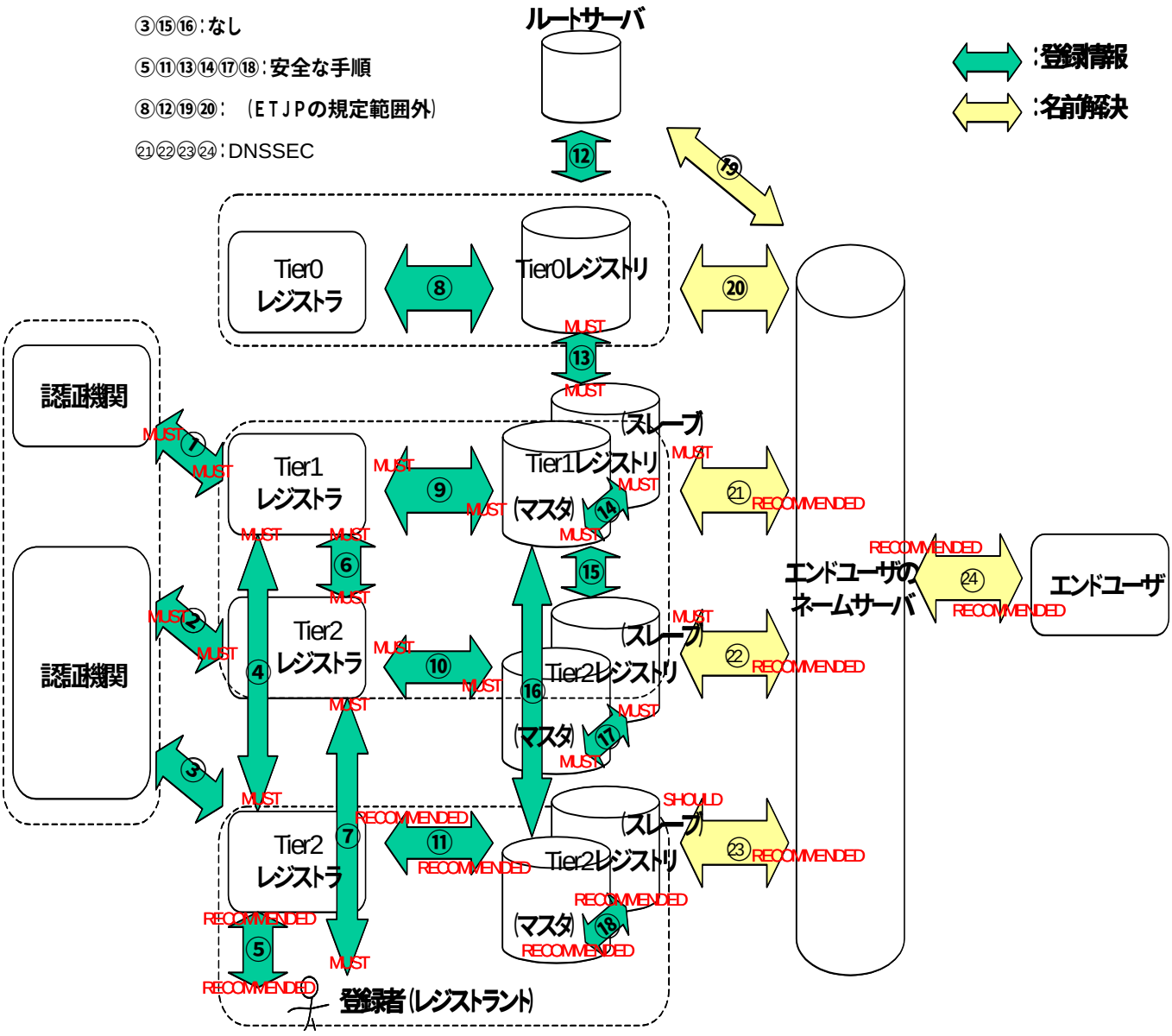
⑥⑨⑩：SSL

③⑮⑯：なし

⑤⑪⑬⑭⑰⑱：安全な手順

⑧⑫⑲⑳：（ETJPの規定範囲外）

㉑㉒㉓㉔：DNSSEC



6-2. ETJP の役割（間）に適用するセキュリティについて(続き)

・④⑥⑦⑨⑩⑬について、ENUM Forum では EPP/HTTPS が規定されることへの検討事項：

－④⑦については、ETJP ではユーザ認証を ID・パスワードベースとし、データ通信路に https を利用しているため、十分なセキュリティを有すると考える
－⑥⑨⑩については、ETJP では同一マシン内にて実装されており、一体運用されるため、通信プロトコルとして SSL で十分と考える
－⑬については、ETJP では JPRS が Tier0/Tier1 ともに ccTLD ゾーンレベルの運用を行っているため、すでに十分な安全性があると考える

・㉑～㉔の名前解決は DNSSEC 対応済みであるが、DNSSEC 実装の普及状況を鑑みて、ユーザサイドでは“RECOMMENDED”扱いとする
・㉓の名前解決についてのサーバサイドの要件は“SHOULD”に設定するが、上記と同様の理由から、各組織においては、DNSSEC 実装の状況に応じて対応するものとする
・⑭⑰については、ENUM Forum では TSIG が規定されるが、ETJP では JPRS が Tier1/Tier2 ともに ccTLD ゾーンレベルの運用を行っているため、すでに十分な安全性があると考える
・⑤⑪⑱については、特段のプロトコル規定は行わないが、ユーザ情報の漏洩、DNS 資源情報の改竄防止について、各組織における十分な検討が行われることが望まれる

7. その他　考慮すべき項目とセキュリティ対応について

（参考：米 ENUM フォーラム ENUM Forum Specification for US implementation of ENUM　P26）

Tier1(&2)DNS(ETJP 事務局保有)について

・物理的対処
　DNS サーバ設置場所の規定/サーバ室への入室人員の制限/
　セキュリティスタッフの配置/他ＬＡＮとの接続制限　など・・・・
・ネットワークのセキュリティ
・バックアップの規定
・セキュリティ監査と報告

→　ETJP トライアルにおいては、
　－会員内実験運用に閉じている
　－レジストリシステム、Tier0/1/2（JPRS 保有）DNS については、物理的には JPRS 担当者以外立ち入ることができない場所において、ｃｃTLD のセキュリティレベルで管理されている
　ため、上記要件のうち、物理的対処の一部とネットワークセキュリティのみを対象としたうえで、これら要件を満足すると考える

Tier2 DNS(会員保有)　について

→前項6-2において記述されるレベルでの運用が行われることで要件を満たすと考える

3.1.2　DNS Working Group

3.1.2.1　設立経緯

ETJP 第三回全体ミーティング（2004 年 1 月 14 日）において、JPRS の藤原和典氏より、日本国内で展開しうる ENUM の DNS モデルを定義し、要求仕様と評価基準を作成し、現在の標準的な DNS 実装を性能評価するための WG を設立することが提案された。同会合にて DNS-WG の設立が合意され、活動を開始した。

3.1.2.2　検討内容

本 WG では、トライアルおよび将来の ENUM の商用利用に向けた基礎データ収集のため、ENUM の利用モデルを想定し、その場合の DNS サーバの負荷について実機検証を行うこととした。具体的には、ENUM DNS の要求仕様・DNS のモデルを規定し、DNS サーバの評価結果を成果として報告することとした。また、名前解決時の改竄等を防ぐため ETJP のトライアルフェーズ 2,3 にて使用が規定された、DNSSEC を使用した場合の性能評価への影響についても当 WG で取り扱うこととなった。

3.1.2.3　要求条件

ENUM の商用利用が見えない現状では、ENUM の利用モデル・前提条件が明確ではない。そこで、トラフィック情報などの数値が公開され、且つ DNS サーバに大規模な負荷がかかる一例として、日本の主要な電話サービスのアドレス解決に ENUM を用いる場合を想定し、ENUM DNS へのエントリ数、DNS の応答性能、DNS のデータ更新頻度などの要求条件を決定した。（参考：「テレコムデータブック 2004」）

3.1.2.3.1 **エントリ数**

固定電話、携帯電話、PHS の加入数・契約数の合計が、平成 14 年度で 1 億 4189 万番号であることから、ENUM DNS へのエントリ数は 1～2 億とする。

3.1.2.3.2 DNS **の応答性能**

固定電話（公衆電話含む)、携帯電話、PHS の総通信回数（総発呼数）は、平成 14 年度で 132,391（百万回）であることから、毎秒の平均発呼数を概算すると 4,000～5,000 呼／秒程度となる。また、固定電話、ISDN の最繁時（9 時～10 時）の発呼数は 6,484（百万回）＝約 4,934 呼／秒であり、携帯電話の最繁時（17 時～18 時）の発呼数は 3,978（百万回）＝約 3,027 呼／秒である。これらの数値は実際には偏りがあると想定されるため、DNS の検索性能としては、輻輳などを考慮し、余裕をみて平均の 10 倍の 50,000query/sec とする。

3.1.2.3.3 DNS のデータ更新頻度（更新に必要な時間）

携帯電話の新規購入や機種変更後に使用可能となるまでの時間を想定し、30 分程度とする。

3.1.2.3.4 要求仕様のまとめ

まとめると以下のようになる。

・エントリ数　　1～ 2 億
・DNS の応答性能　5 万 query/sec
・DNS のデータ更新頻度　30 分

3.1.2.4 ENUM DNS のモデル

「ENUM 研究グループ報告書」（2003 年）p23,24 にて規定された(1) から(4) の ENUM DNS のモデルを前提とする。ここで、本検討においては、ETJP のトライアルにおいて、
・Tier1,2 の ENUM DNS サーバが分離している
・Tier1 サーバの分離は想定されていない
ことを踏まえ、(1)と(4)を対象外とし、(2) と(3) を検討する。

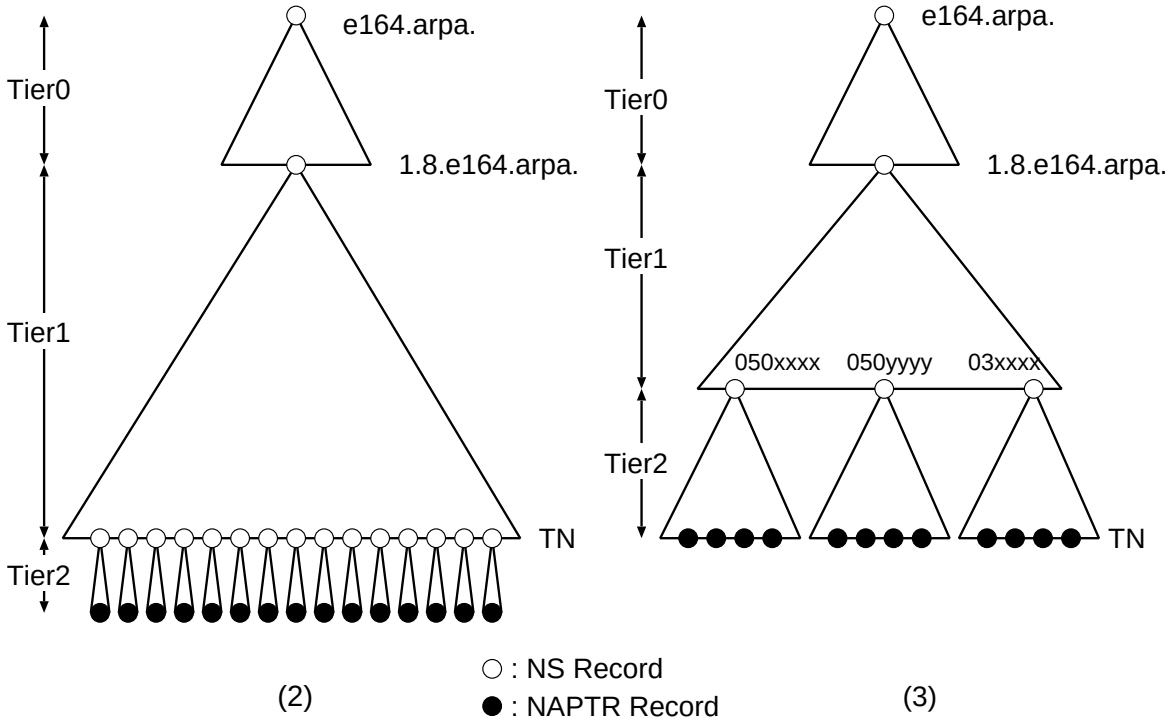


図 1 DNS-WG で対象とする ENUM DNS の Tier 構造

以下、便宜的に(2)を局番単位モデル(Number Allocation Model)、(3) をたけのこモデル(Takenoko Model) と呼ぶ。

3.1.2.5 DNS サーバの評価

3.1.2.5.1 **総論**

3.1.2.3、3.1.2.4 にて整理した要求条件、モデルについて、一台のマシンでの性能を測定し、実用的な台数組み合わせて実現できる構成を求めることとした。(一般的に、実用的に運用可能な台数は、DNS を運用する組織あたり 10 から 100 程度であると考えられる。) 測定の結果、DNSSEC を考慮しない場合には、現在入手可能なマシンを実用的な台数組み合わせることにより、今回の要求条件を満足する形で各モデルを構成できる可能性があることが分かった。

(注 : 本検討は特定のマシンスペック、OS 等の前提条件による測定結果から得られる一考察であり、実際のシステム構築にあたっては、個別の検討が必要と思われる)

また、DNSSEC を考慮した場合の性能評価については、今後検討することとした。

3.1.2.5.2 評価方法

二つのモデル、それぞれの Tier1、Tier2 計 4 パターンについて、想定される DNS ゾーンファイルを作成し、単体 DNS サーバの評価を行なった。スケーラビリティの評価を行なうため、エントリ数を変化させ、さまざまなサイズのデータを生成した。測定した項目は、メモリ使用量、読み込み時間、再読み込み時間、サーバの応答性能である。それぞれの DNS データファイルごとに、現在多く使用されている複数の DNS サーバでの性能を測定した。評価基準としてのエントリ数、パフォーマンスはわかりやすいが、更新条件を判断する基準として、30 分更新を実現するためには半分の 15 分以内に再読み込みできないと実現困難であるため、再読み込みが 15 分で完了することを実現可能性の判断基準とする。以下にそれぞれの項目を詳細に説明する。

3.1.2.5.2.1 評価に使用した DNS ゾーンファイル

測定条件を簡単にするため、国内に割り当てる ENUM 用電話番号の桁数を 10 桁と仮定した。050 番号や携帯電話の番号は、先頭の 0 を除くと 10 桁であるため、この仮定は妥当である。また、測定をやりやすくするため、各モデルでは 0000000000 から順に番号を使うこととした。また、局番単位モデルでは、局番ごとに 10000 番号の割り振りを行なうこととし、Tier1 で 6 桁、Tier2 で 4 桁の展開を行なうこととする。

3.1.2.5.2.1.1 局番単位モデル Tier1

4 桁分を管理する局番ごとに、Tier2 に委任を行なうが、それぞれ 2 つのネームサーバを指定すると仮定した。エントリ数を指定してデータファイルを指定する。ネームサーバ名は ns1.isp0XX.jp, ns2.isp0XX.jp とした。XX は 00 から 99 までの数で、局番の下 2 桁と同じである。

局番単位モデル Tier1 ゾーンファイル　10 局番の場合

```
$ORIGIN 1.8.e164.arpa.
$TTL 120
@ IN SOA ns0.etjp.jp. postmaster.etjp.jp. (1 1H 5M 7D 10M)
 IN NS ns1.etjp.jp.
 IN NS ns2.etjp.jp.

0.0.0.0.0.0 IN NS ns1.isp000.jp.
```

```
0.0.0.0.0.0 IN NS ns2.isp000.jp.
1.0.0.0.0.0 IN NS ns1.isp001.jp.
1.0.0.0.0.0 IN NS ns2.isp001.jp.
(中略)
9.0.0.0.0.0 IN NS ns1.isp009.jp.
9.0.0.0.0.0 IN NS ns2.isp009.jp.
```

3.1.2.5.2.1.2 局番単位モデル Tier2

4 桁分、10000 番号ごとに委任を受け、ゾーンファイルを提供する。ゾーンの内容として、SOA、ネームサーバ 2 台として NS 2 行、適当な SIP URI を返す NAPTR を 10000 行記述した。また、一台のネームサーバで複数のゾーンを管理するため、複数のゾーンを読む named.conf を生成した。

局番単位モデル Tier2 ゾーンファイル (10000 番号分)

```
$ORIGIN 0.0.0.0.0.0.1.8.e164.arpa.
$TTL 120
@ IN SOA ns1.etjp.jp. postmaster.etjp.jp. (1 1H 5M 7D 10M)
 IN NS ns1.etjp.jp.
 IN NS ns2.etjp.jp.
0.0.0.0 IN NAPTR 100 0 "u" "E2U+sip" "!^.*$!sip:00000000@sipisp.jp!" .
1.0.0.0 IN NAPTR 100 0 "u" "E2U+sip" "!^.*$!sip:00000001@sipisp.jp!" .
(中略)
9.9.9.9 IN NAPTR 100 0 "u" "E2U+sip" "!^.*$!sip:00009999@sipisp.jp!" .
```

局番単位モデル Tier2 named.conf　100 ゾーンの場合

```
options {
  ..
};

zone "0.0.0.0.0.0.1.8.e164.arpa." {
 type master; file "0.0.0.0.0.0.1.8.e164.arpa."; };
zone "1.0.0.0.0.0.1.8.e164.arpa." {
 type master; file "0.0.0.0.0.0.1.8.e164.arpa."; };
(中略)
```

```
zone "9.9.0.0.0.0.1.8.e164.arpa." {
  type master; file "0.0.0.0.0.0.1.8.e164.arpa."; };
```

3.1.2.5.2.1.3 たけのこモデル Tier1

一つの番号ごとに Tier2 に委任を行なうが、それぞれ 2 つのネームサーバを指定すると仮定した。エントリ数を指定してデータファイルを指定する。ネームサーバ名は ns1.isp0XX.jp, ns2.isp0XX.jp とした。XX は 00 から 99 までの数で、番号そのものの下 2 桁と同じである。

たけのこモデル Tier1 ゾーンファイル　123456790 番号の場合

```
$ORIGIN 1.8.e164.arpa.
$TTL 120
@ IN SOA ns1.etjp.jp. postmaster.etjp.jp. (1 1H 5M 7D 10M)
   IN NS ns1.etjp.jp.
   IN NS ns2.etjp.jp.

0.0.0.0.0.0.0.0.0.0 IN NS ns1.isp000.jp.
0.0.0.0.0.0.0.0.0.0 IN NS ns2.isp000.jp.
1.0.0.0.0.0.0.0.0.0 IN NS ns1.isp001.jp.
1.0.0.0.0.0.0.0.0.0 IN NS ns2.isp001.jp.
(中略)
9.8.7.6.5.4.3.2.1.0 IN NS ns1.isp089.jp.
9.8.7.6.5.4.3.2.1.0 IN NS ns2.isp089.jp.
```

3.1.2.5.2.1.4　たけのこモデル Tier2

一つの番号ごとに委任を受け、ゾーンファイルを提供する。ゾーンの内容として、SOA、ネームサーバ 2 台として NS 2 行、適当な SIP URI を返す NAPTR を 1 行記述した。また、一台のネームサーバで複数のゾーンを管理するため、複数のゾーンを読む named.conf を生成した。

たけのこモデル Tier2 ゾーンファイル (1 番号分)

```
$ORIGIN 0.0.0.0.0.0.0.0.0.0.1.8.e164.arpa.
$TTL 120
```

```
@ IN SOA ns1.etjp.jp. postmaster.etjp.jp. (1 1H 5M 7D 10M)
   IN NS ns1.etjp.jp.
   IN NS ns2.etjp.jp.
   IN NAPTR 100 0 "u" "E2U+sip" "!^.*$!sip:00000000@sipisp.jp!" .
```

たけのこモデル Tier2 named.conf (100 番号の場合)

```
options {
  ..
};

zone "0.0.0.0.0.0.0.0.0.0.1.8.e164.arpa." {
  type master; file "00000/0.0.0.0.0.0.0.0.0.0.1.8.e164.arpa."; };
zone "1.0.0.0.0.0.0.0.0.0.1.8.e164.arpa." {
  type master; file "00000/1.0.0.0.0.0.0.0.0.0.1.8.e164.arpa."; };
(中略)
zone "9.9.0.0.0.0.0.0.0.0.1.8.e164.arpa." {
  type master; file "00000/9.9.0.0.0.0.0.0.0.0.1.8.e164.arpa."; };
```

3.1.2.5.2.2 測定項目

合理的に ENUM DNS サービスを提供できるかどうかを判断するためには、現実に存在するサーバマシンを用いて、データを保持できること、許される時間でデータを読み込めること、そのときに所定の応答性能を得られることを調べる必要がある。また、更新時間の制約もあるため、再読み込み時間も測定した。

メモリサイズは、DNS サーバがデータを読み込んだ後のプロセスサイズを測定した。再読み込みを行なう際には二倍のメモリを必要とする実装があるが、考慮していない。

読み込み時間は、DNS サーバを起動してから、DNS サービスを提供するまでにかかる時間を測定した。再読み込み時間は、再読み込み指示を出してから、新しいデータを提供するまでの時間とした。テキストファイル形式のデータを別プログラムで内部形式に変換する必要がある DNS サーバソフトウェアの場合は、読み込み・再読み込み時間にそれぞれ変換時間を加えた。

応答性能は、BIND 9 に附属する queryperf というソフトウェアを用い、存在するドメイン名に対する NAPTR 問い合わせを 20 秒行ない、どれだけの応答がもどっ

てきたかで評価した。単位は qps(query per second)である。再読み込みで性能が遅延するソフトウェアの場合は、その場合の性能も測定した。

3.1.2.5.2.3 評価した DNS サーバ

今回は、よく使用されている実装として、BIND 8 と BIND 9、NSD、djbdns を評価した。BIND 8 は ISC が開発しており、従来の標準であるが、再読み込み中に無応答になるなど、古い実装である。今回は IPv6 対応機能を持たない最新版である 8.3.7 を評価した。BIND 9 は ISC が参照実装として開発しており、DNSSEC などの最新機能に対応している。今回は最新の 9.3.0 を評価した。NSD は、ヨーロッパの NL NetLabs と RIPE NCC が開発しており、ゾーンデータを提供する機能に特化している。こちらも DNSSEC に対応している。NSD は 2.1.2 で採り入れられたデータ整合性チェック機能の負荷が大きいため、2.1.1 を用いて評価を行なった。djbdns は、数学者の D. J. Bernstein 助教授が安全性と完全性にこだわって開発しているもので、比較的小さく安定的に開発されている。ENUM で使用する機能については、作者がまだ必要と考えていないため入っていないが、周囲の開発者により、patch の形で提供されている。今回は version 1.05 に、NAPTR+SIP パッチと、性能向上パッチをあてたものを評価した。djbdns の場合、テキストデータをバイナリデータに変換する必要はあるが、データベース入れ換えは mv でファイルを入れ換えるだけで完了するため、データ入れ換え時間はゼロであり、特殊な負荷は発生しない。

3.1.2.5.2.4 測定手順

測定対象となる DNS サーバ PC と、性能測定を行なう負荷生成 PC を用意し、その間を Ethernet で接続する。

DNS サーバ PC-------Ethernet-------測定用 PC

3.1.2.5.2.1 で説明したゾーンファイルを DNS サーバ PC に置き、そこでネームサーバソフトウェアを起動し、読み込み時間、メモリ使用量を測定し、測定用 PC から queryperf で負荷をかけ、応答性能を測定した。次に DNS サーバ PC にてゾーンファイルを再読み込みさせ、負荷をかけない場合の再読み込み時間を測定した。さらに、もう一度 DNS サーバ PC にてゾーンファイルを再読み込みさせ、測定用 PC から queryperf で負荷をかけ、再読み込み中の応答性能を測定した。

3.1.2.5.2.5 Tier1 BIND9 性能改善

次章の測定結果 3.1.2.5.3.1, 3.1.2.5.3.3 で示すが、局番単位モデル・たけのこモデル Tier1 の場合、BIND 9 では性能が全くでない。これは BIND9 の内部構造と推測され、ISC 開発担当者に質問をしたところ肯定され、階層が深い ENUM 型ゾーンファイルをそのまま持たせると性能が出ないことがわかった。解決方法として、図 11 のように 4 桁程度で階層を分割し、分割したすべてのゾーンファイルを一台に持たせることとした。同様に、局番単位モデルにおいても BIND 9 用のゾーンファイルを作成し、評価を行なった。

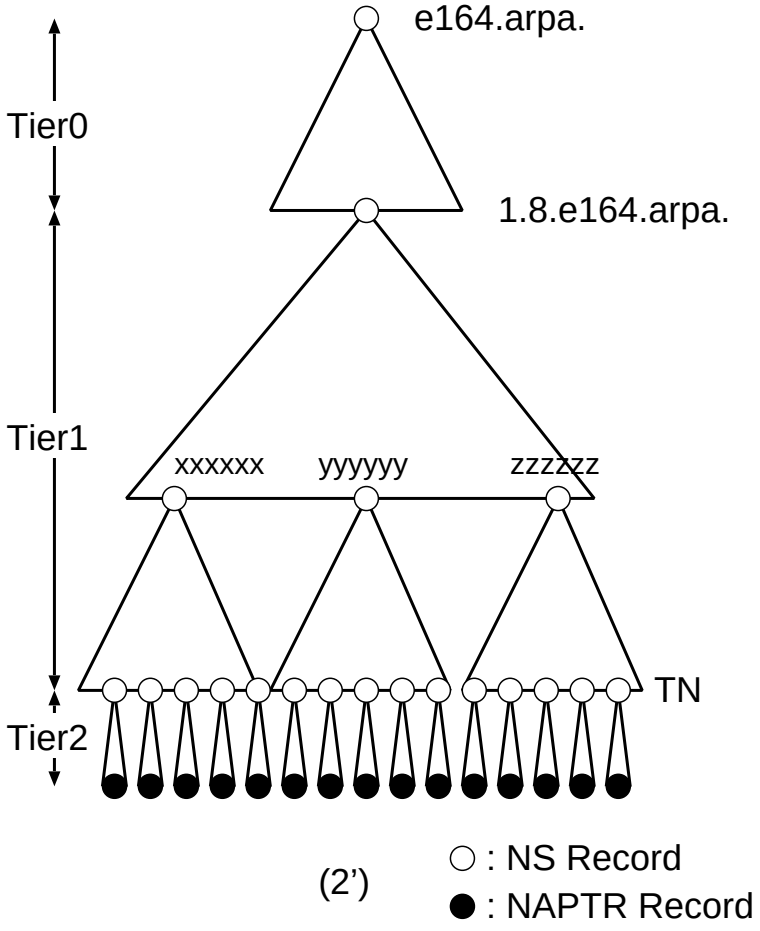


図 2 たけのこモデル Tier1 BIND9 性能改善案

たけのこモデル Tier1 で 8 桁の 1000 万エントリゾーンの場合、下位 4 桁 10000 エントリのゾーン 1000 個に分割し、一台にすべてのゾーンを持たせる。また、局番単位モデル Tier1 で 6 桁の 100 万エントリゾーンの場合、下位 4 桁一万エントリのゾーン 100 個に分割し、一台にすべてのゾーンを持たせる。3.1.2.5.3 測定結果 1 では bind9+ として表している。

3.1.2.5.3 **測定結果** 1

DNS-WG 有志三者により測定を行なった。マシン環境や OS などの条件は異なったが、おおむね傾向が同じであったため、一者の測定結果を示す。

以下、局番単位モデル Tier1、局番単位モデル Tier2、たけのこモデル Tier1、たけのこモデル Tier2 それぞれに、保持するドメイン数を変化させたときのメモリ使用量、応答性能、読み込み時間、再読み込み時間を図示した。それぞれ、BIND 8、BIND 9、bind9+(Tier1 のみ)、djbdns、NSD の比較を行なっている。それぞれ、横軸は保持するドメイン名数で、対数スケールとしている。また、グラフ A の縦軸はメモリ使用量で単位はメガバイト、グラフ B の縦軸は応答性能(秒あたりの応答数)、グラフ C・D の縦軸は読み込み・再読み込み時間で、単位は秒であり、対数スケールである。

測定対象 DNS サーバには、Pentium4-3GHz、メモリ 2.5GB の PC を用い、OS として FreeBSD 4.10-RELEASE を導入した。負荷生成マシンには、Pentium4-2.7GHz、メモリ 512MB の PC を用い、OS として FreeBSD 4.10-RELEASE を導入した。2 台の間を 100baseTX の switch を用いて接続した。これらのマシンは 2004 年現在、標準的な PC であり、DNS サーバ PC には大きめのデータがのせられるように、すこしだけ多めにメモリをつんでいる。

3.1.2.5.3.1 局番単位モデル Tier1 評価

割り当て単位モデル Tier1 では、全電話番号空間を 10 桁と仮定しているため、最大 6 桁、100 万の権限委任を保持できればよい。各委任ごとにネームサーバ 2 台と仮定しているため、ゾーンファイルは 200 万行となる。評価結果を図 11 に示す。

図 11[A]によると、メモリ使用量はエントリ数に比例しているが、最大の 100 万エントリの場合でも 200M バイト以下であり、再読み込み時に 2 倍となっても問題がない。

次に、図 11[B]によると、NSD と BIND 8 の場合はどの場合でも 37000qps 以上の性能を出している。BIND 9 の場合は、そのままではエントリ数が増えるに従い、著しく性能が低下するが、BIND 9 用に最適化したデータを作成すると 10000qps 以上のよい性能を出せることがわかる。また djbdns の場合も 6000qps 以上の性能を得られている。

データ読み込み時間について、図 11[C]によると一番遅い NSD の場合でも、100 秒以内、図 3[D]の再読み込み時間を見ると、BIND 9 をそのまま使った場合に 1600 秒か

かるが、BIND 9 用に最適化すると 100 秒以内となる。

再読み込み中の性能は、図 11[B]によると、NSD で最大半分に、BIND 9 では 2 割程度にまで落ちることがわかる。また BIND 8 では無応答になるので、複数のサーバを用意し、再読み込みタイミングをずらすなどの対応が必要である。

全体として、局番単位モデル Tier1 では、そのモデルそのままの形でサーバにデータを保持することができ、さらに、BIND 8、NSD の場合は 2 台以上、BIND 9 の場合で 5 台以上、djbdns の場合 9 台以上を並列に用いることで条件を満たせることがわかる。

3.1.2.5.3.2 局番単位モデル Tier2 評価

割り当て単位モデルでは、それぞれの Tier2 事業者は複数の一万番号ゾーンを管理する。今回は 1000 ゾーンまでの評価を行なった。評価結果を図 12 に示す。

図 4[A]によると、メモリ使用量はゾーン数に比例しており、1000 ゾーンの場合には 1G バイトから 2G バイトのメモリを使用する。特に NSD が再読み込みを行なう場合、動作時の倍のメモリを使用するため、今回の条件では、NSD で 1000 ゾーンの保持は困難であることがわかる。

次に、図 4[B]によると、BIND 8 では 36000qps、NSD では 500 ゾーンまで 37000qps の性能を出している。BIND 9 でも 1 万 qps 前後の性能を出している。djbdns は 1000 ゾーンで 4600qps 程度の性能である。NSD の場合、メモリを十分に用意してあれば、十分な性能が得られると考えられる。

データ読み込み時間について、図 4[C]によると、NSD の場合、1000 ゾーンで 1362 秒とかなり多くの時間がかかっている。500 ゾーンまでであれば 573 秒と実用的である。また、他のソフトウェアではどれでも 1000 ゾーンで 120 秒以下であり、実用的である。

図 4[D]によると、再読み込み時間は、NSD の場合は読み込み時間と一致している。また BIND 8 や BIND 9 の場合も、再読み込みのほうが時間がかかるが、形は類似している。BIND 9 の場合、おおむね読み込みの倍の時間がかかる。

再読み込み中の性能は、図 4[B]によると、NSD で 4 割程度に、BIND 9 では 15%程度にまで落ちることがわかる。また BIND 8 では無応答になるので、複数のサーバを

用意し、再読み込みタイミングをずらすなどの対応が必要である。

全体として、局番単位モデル Tier1 では、一台のシステムで 500 から 1000 ゾーンを保持、つまり 500 万〜1000 万番号を扱え、さらに、BIND 8、NSD の場合は 2 台以上、BIND 9 の場合で 6 台以上、djbdns の場合 12 台以上を並列に用いることで性能条件を満たせることがわかる。NSD の場合は 500 ゾーン程度以下で運用すれば更新頻度条件を満たせ、それ以外では 1000 ゾーンでも満たせる可能性がある。

3.1.2.5.3.3 たけのこモデル Tier1 評価結果

たけのこモデル Tier1 では、全電話番号空間 10 桁中の各番号への権限委任を保持する。1 億番号を目標とするが、今回は 100 万から 2000 万番号の間での評価を行なった。1000 万番号の場合、各委任ごとにネームサーバ 2 台と仮定しているため、ゾーンファイルは 2000 万行となる。評価結果を図 5 に示す。

図 5[A]によると、メモリ使用量はエントリ数に比例している。今回テストを行なった環境の実メモリが 2.5G バイトであり、2G を越えると性能が劣化することより、実装によるが 1000 万番号をすこし越えたところに上限がある。

そこで、今回の目標を、1 億を 10 システムに分割し、1000 万番号システムを運用できることを検証することとする。同一の運用者が 10 システムを統一的に運用すれば、1 億番号のシステムを一つ運用することと等価である。

次に、図 5[B]によると、1000 万番号以内では、NSD と BIND 8 では 30000qps 以上、BIND 9 では BIND 9 用に最適化した場合に 10000qps 程度の性能を維持できている。djbdns は 700 万番号までは 7700qps の性能を維持できているが、1000 万番号で落ちている。BIND 9 をそのまま用いると全く性能が出ていない。

図 5[C]によると、データ読み込み時間は、NSD の場合には 26 分かかるが、BIND8、BIND 9 の場合は 5 分以内で読み込めている。図 5[D]によると、データ再読み込み時間は、NSD の場合には読み込み時間とほぼ同じ 27 分かかるが、BIND 8、BIND 9 の場合は読み込み時間と同様に 5 分以内で読み込めている。

図 5[B]によると、再読み込み中の性能は、NSD で 4 割に、BIND 9 では 2 割弱にまで落ちることがわかる。また BIND 8 では無応答になる。どのサーバの場合でも、複数のサーバを用意し、再読み込みタイミングをずらすなどの対応が必要である。

全体として、たけのこモデル Tier1 では、BIND 8、NSD の場合は 2 台以上、BIND9 の場合で 6 台以上用いることで 1000 万番号の場合はほぼ要件を満たせるが、再読み込み時の性能に注意する必要があること、NSD の場合の再読み込みの設計に注意が必要である。また、NSD では再読み込み時間が基準の倍と大き過ぎる。

3.1.2.5.3.4 たけのこモデル Tier2 評価

たけのこモデルでは、それぞれの Tier2 事業者は番号一つずつのゾーンを管理する。今回は 500 万ゾーンまでの評価を行なった。評価結果を図 6 に示す。

まず、BIND 8、BIND 9 では、100 万ゾーンを保持させようとしたところ、一時間で終らなかったため、データをとることを断念した。NSD、djbdns の場合、技術的関心から時間制限を加えず、500 万ゾーンまでの測定を行なった。

図 6[A]によると、メモリ使用量はゾーン数に比例しており、NSD、djbdns の 500 万ゾーンの場合には 2G バイトから 3G バイトのメモリを使用する。また、BIND 9 の場合、50 万ゾーンであれば 1.5G バイトで保持できる。

次に、図 6[B]によると、NSD、BIND 8 ではデータを保持できた範囲で 30000qps 以上、djbdns では 100 万ゾーンまで 3400qps であるが、500 万ゾーンでは 146qps と性能が飽和している。BIND 9 は 50 万ゾーンで 356qps と全く性能が出ていない。

データ読み込み時間について、図 6[C][D]によると、NSD の場合、500 万ゾーンで 4879 秒、再読み込みに 5048 秒とかなり多くの時間がかかっている。100 万ゾーンまでであればそれぞれ 804 秒、741 秒と、実用的と考えられる時間で読み込み・再読み込みできている。djbdns の場合、100 万ゾーンで 68 秒、500 万ゾーンで 361 秒と短時間でデータの更新が可能である。BIND の場合、50 万ゾーンでも BIND 8 で 2000 秒、BIND 9 で 4000 秒の読み込み時間がかかり、実用的でないが、再読み込みの場合、変化のあったゾーンのみ読み込むため、実際の運用では比較的短時間で再読み込みが終る可能性がある。

再読み込み中の性能は、図 6[B]によると、NSD で 4 割程度に落ちる。また BIND8 では無応答になるので、複数のサーバを用意し、再読み込みタイミングをずらすなどの対応が必要である。

全体として、たけのこモデル Tier2 では、NSD を用いることにより、一台のシステムで 100 万ゾーンを管理することが可能であり、2 台のサーバを用いることにより、

50000qps を達成できる。

3.1.2.5.3.5 測定結果 1 まとめ

局番単位モデルは、たとえば BIND 9 を用い、各サーバを 6 台のマシンで負荷分散することで、1 システムで Tier1 を構成でき、1000 ゾーンを管理する Tier2 10 システムですべての Tier2 を構成できる。

たけのこモデル Tier1 は、局番単位モデルと同様に、たとえば BIND 9 を用い、各サーバを 6 台のマシンで負荷分散し、さらに 8 桁の一億番号空間を 1000 万番号空間 10 個に分割することで実現できる。

たけのこモデル Tier2 は、NSD を用いることにより、1 システム 2 台で 100 万番号をサポートする Tier2 を構成でき、これを 100 システム用いることで一億番号を保持できる。

全体として、DNSSEC を考慮しない場合には、実用的な台数で各モデルを構成できることがわかった。

3.1.2.5.4 **測定結果** 2

ENUM の商用利用時には、ENUM の番号が新たに追加されてもユーザへのクエリ応答を中断することはできない。実運用では、絶えずユーザに対してクエリ応答が行なわれ、また番号の登録・削除も同時に行われることになる。番号の登録・削除を行った場合、DNS サーバへの反映を行う手段の１つとして再読み込み（リロード）が必要になる。

そこで本章では、

・DNS の応答性能が、リロードの有無によってどのような傾向を示すか、

・リロード時間が、クエリ負荷の有無によってどのような変化を示すか

について測定することとした。

また参考として読み込み時と再読み込み時のメモリ使用量に変化がないかについても測定を行った。

測定方法、各モデルのデータ構成は、3.1.2.5.3 と同様の条件とし、3.1.2.5.3 の結果からエントリ数は各モデル毎 2 つのポイントで測定を行った。

なお本測定は、5.1.2.5.3 と異なるハード、OS 条件で実施したため簡単に差分を示す。

【測定条件】

・DNS サーバ：SUN Fire V65x
CPU：Intel Xeon 2.8GHz x 1 個
Memory：4.5GB
OS：SUN Solaris9(x86)
DNS：BIND9 rc4

・性能測定用 PC
CPU：Intel Xeon 3.2GHz x 1 個
Memory：6.0GB
OS：LinuxRH9
性能測定用アプリケーション：QueryPerf

3.1.2.5.4.1 局番単位モデル Tier1 評価

エントリ数は、10 万エントリと、100 万エントリで測定を行った。
図 7[A]によると、リロードの有無による DNS の応答性能は、10 万エントリで、リロード中は約 25%の性能劣化があった。また 100 万エントリでは、リロード実施していない状態でも性能があまりでていないため大きな差にはならなかった。
図 7[B]によると、クエリ負荷の有無によるリロード時間は、10 万エントリでは、元々のリロード時間が短いため差は見受けられないが、100 万エントリでは、クエリ負荷有の場合、約 8.5 倍の時間を要している。
図 7 [C]によると、メモリ使用量は、リロードすることによって両エントリとも約 2 倍必要となっている。

3.1.2.5.4.2 **局番単位モデル** Tier2 **評価**

エントリ数は、100 万エントリと、500 万エントリで測定(BIND9+)を行った。

図 8[A]によると、リロードの有無による DNS の応答性能は、両エントリともリロード中は約 65%の性能劣化があった。
図 8[B]によると、クエリ負荷の有無によるリロード時間は、両エントリともクエリ負荷有の場合、約 1.5 倍以上の時間を要している。
図 8[C]によると、メモリ使用量は、リロードしても両エントリともほとんど差が見られなかった。

3.1.2.5.4.3 たけのこモデル Tier1 評価

エントリ数は、100 万エントリと、500 万エントリで測定を行った。
図 9[A]によると、リロードの有無による DNS の応答性能は、両エントリともリロード中は約 65%の性能劣化があった。
図 9[B]によると、クエリ負荷の有無によるリロード時間は、両エントリともクエリ負荷有の場合、約 1.5 倍以上の時間を要している。
図 9[C]によると、メモリ使用量は、リロードしても両エントリともほとんど差が見られなかった。

3.1.2.5.4.4 たけのこモデル Tier2 評価

エントリ数は、10 万エントリと、30 万エントリで測定を行った。
図 10[A]によると、リロードの有無による DNS の応答性能は、10 万エントリで、リロード中は約 35%また 30 万エントリでは、約 60%の性能劣化があった。
図 10[B]によると、クエリ負荷の有無によるリロード時間は、両エントリともクエリ負荷有の場合、約 1.2 倍以上の時間を要している。
図 10[C]によると、メモリ使用量は、リロードすることによって両エントリとも約 1.4 倍必要となっている。

3.1.2.5.4.5 測定結果 2 のまとめ

局番単位モデル Tier2 とたけのこモデル Tier1 は、ゾーンの分割方法、１ゾーンあたりのエントリ数が似ているため同様の測定結果となっている。

全ての番号を１ゾーンで管理している局番単位モデル Tier1 は、リロード時間に大きな影響があった。またメモリ使用量が 2 倍近く必要になることも注意すべき点である。

局番単位モデル Tier2 とたけのこモデル Tier1 は、DNS の応答性能、リロード時間ともに無視できない影響がある。

たけのこ Tier2 の場合、無負荷状態でもリロード時間は他のモデルと比べて非常に長いため増加率としては小さく見えても実時間としては注意が必要である。また応答性能もリロードがない状態でも他のモデルに比べて性能はでないので同様に注意が必要である。

今回の測定は、各モデルとも測定ポイントが少ないことから、エントリ数を変えて測定すると比率的には変動する可能性が高い。また BIND9 の特性や、OS の CPU の割当ての影響も十分考えられる。本報告では割愛するが、同一マシンを 2CPU にした場合、同一の測定を行っても異なる結果となっている。

実際に ENUM が運用され始めた後は、番号のデータ更新方法としては、今回測定を行ったリロードを用いる方法、差分だけを反映する差分ゾーン転送を用いる方法などいくつかの方法が考えられる。また 3.1.2.5.3 の結果からわかるように使用する DNS 製品によっても特性は大きく異なる。

ただし実際の運用では絶えずユーザからのクエリが通知され、同時に番号の追加・変更・削除が頻繁に行われるためリロード中の DNS 応答性能、リロード時間を考慮して設備設計する必要がある。

3.1.2.6 結論

今回の性能評価結果から、日本全国規模で ENUM を展開することを考えた場合、現在入手可能なマシンを実用的な台数組み合わせ、各モデルを構成できることを概ね確認することができた。また使用する DNS 実装によって応答性能、読み込み時間、メモリ使用量が異なり、またそれぞれの結果に因果関係があることも明らかになった。

ENUM の商用利用を考えた場合、さらに考慮すべき要素が増える可能性はあるが今回の DNS-WG の活動を通して、主な要求仕様と評価基準は確立されたと考える。

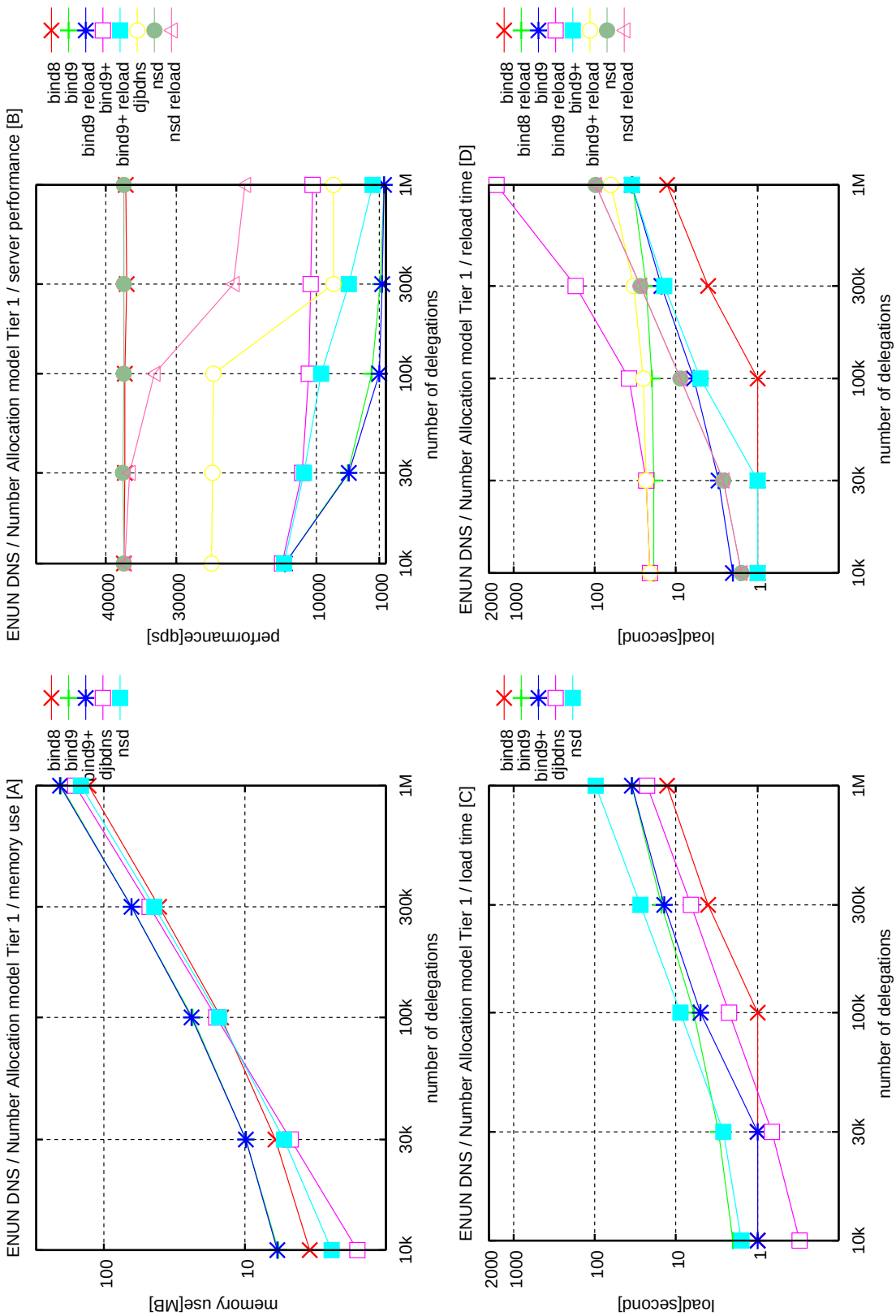


図 3 局番単位モデル Tier1 評価結果

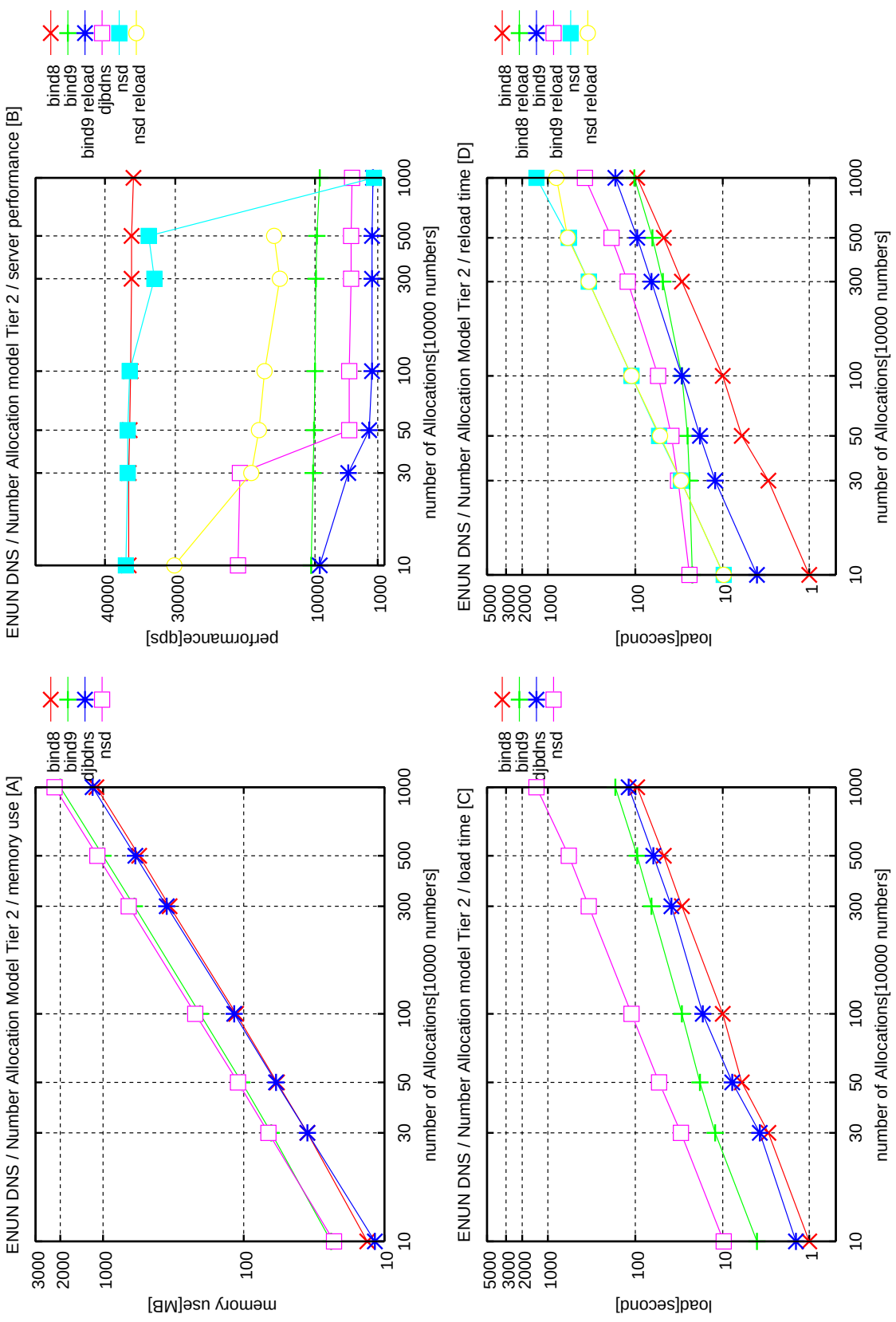


図 4 局番単位モデル Tier2 評価結果

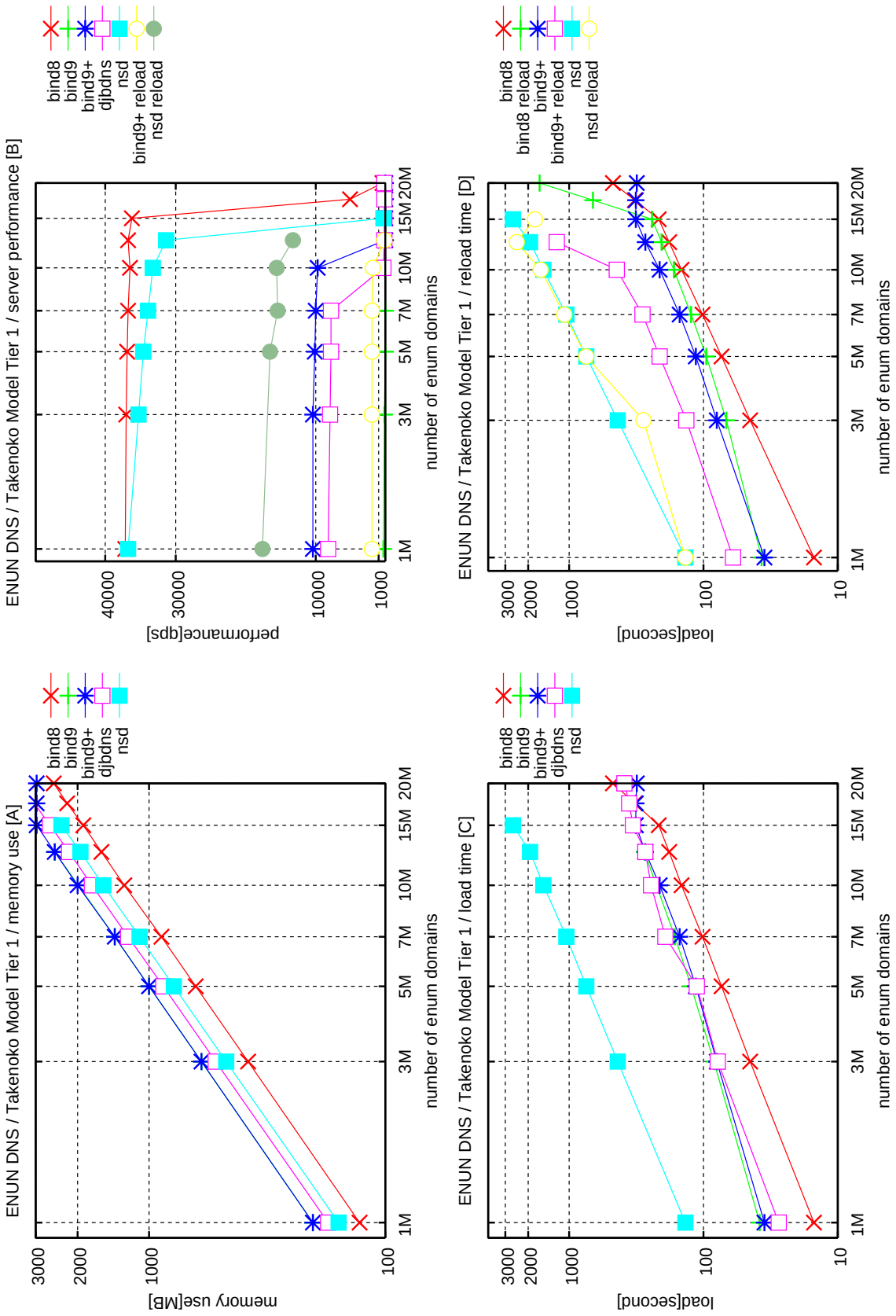


図 5 たけのこモデル Tier1 評価結果

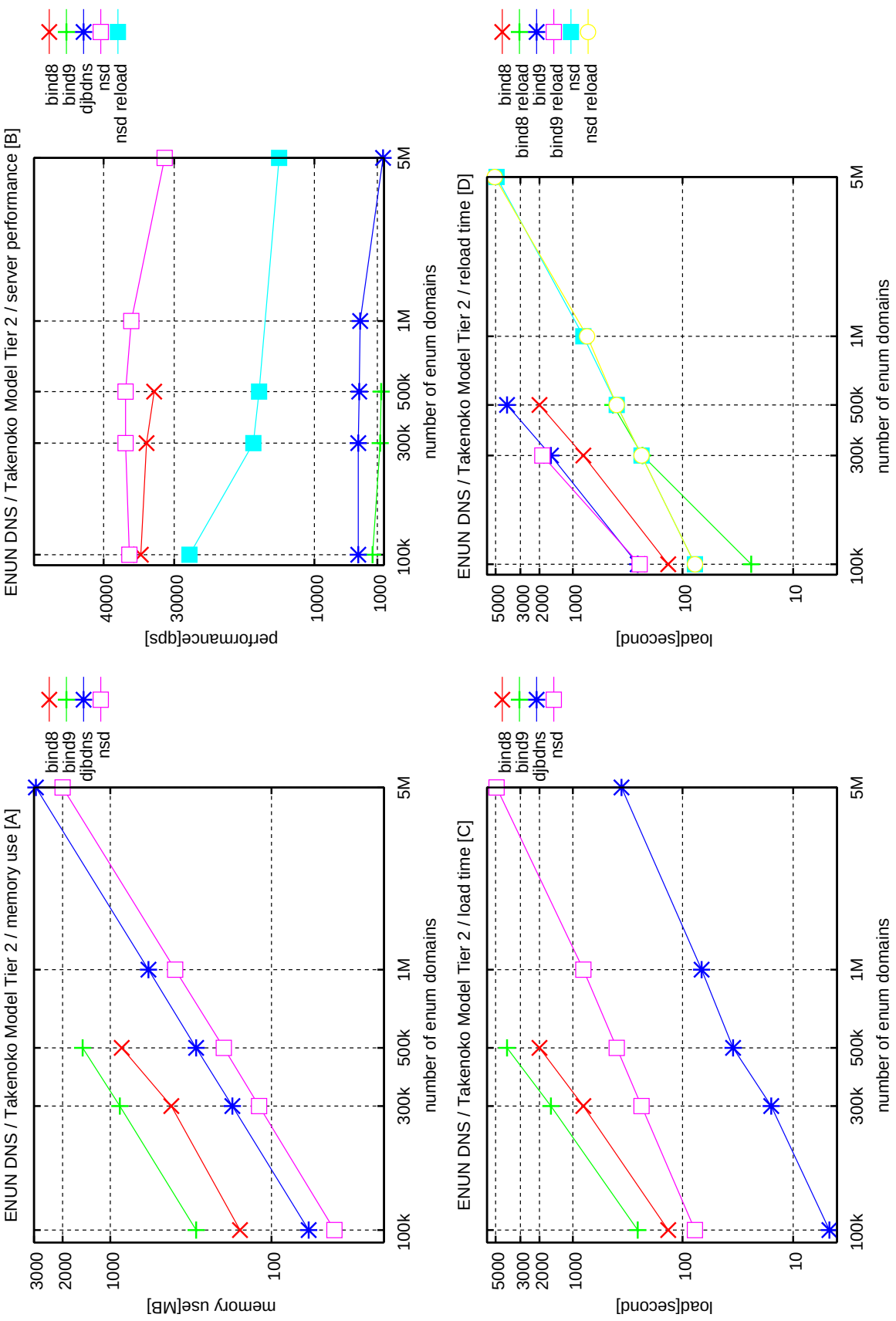


図 6 たけのこモデル Tier2 評価結果

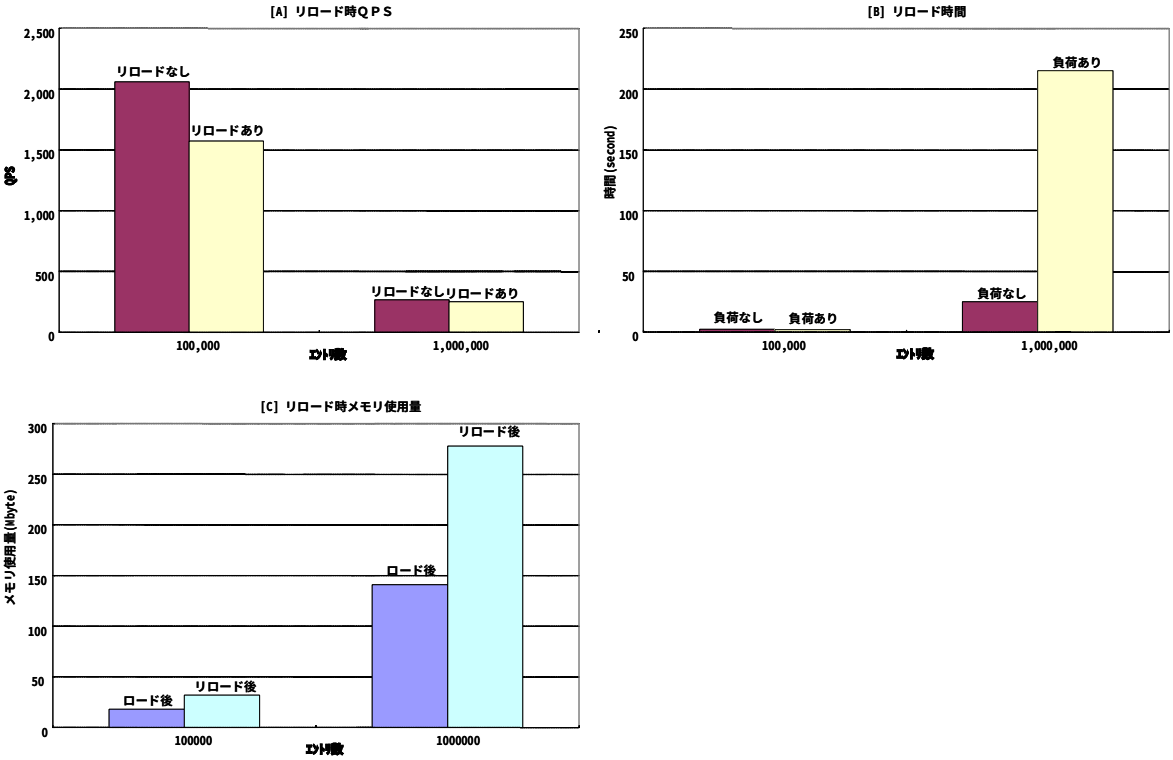


図 7 局番単位モデル Teir1 評価結果

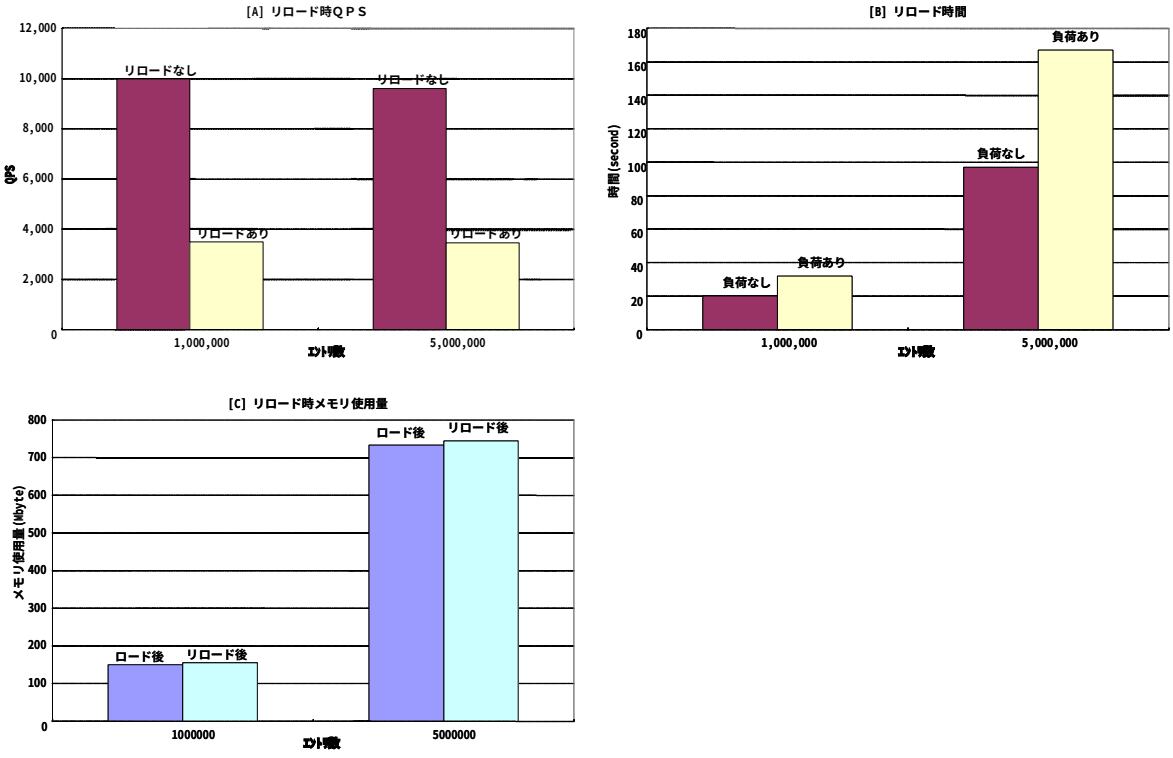


図 8 局番単位モデル Teir2 評価結果

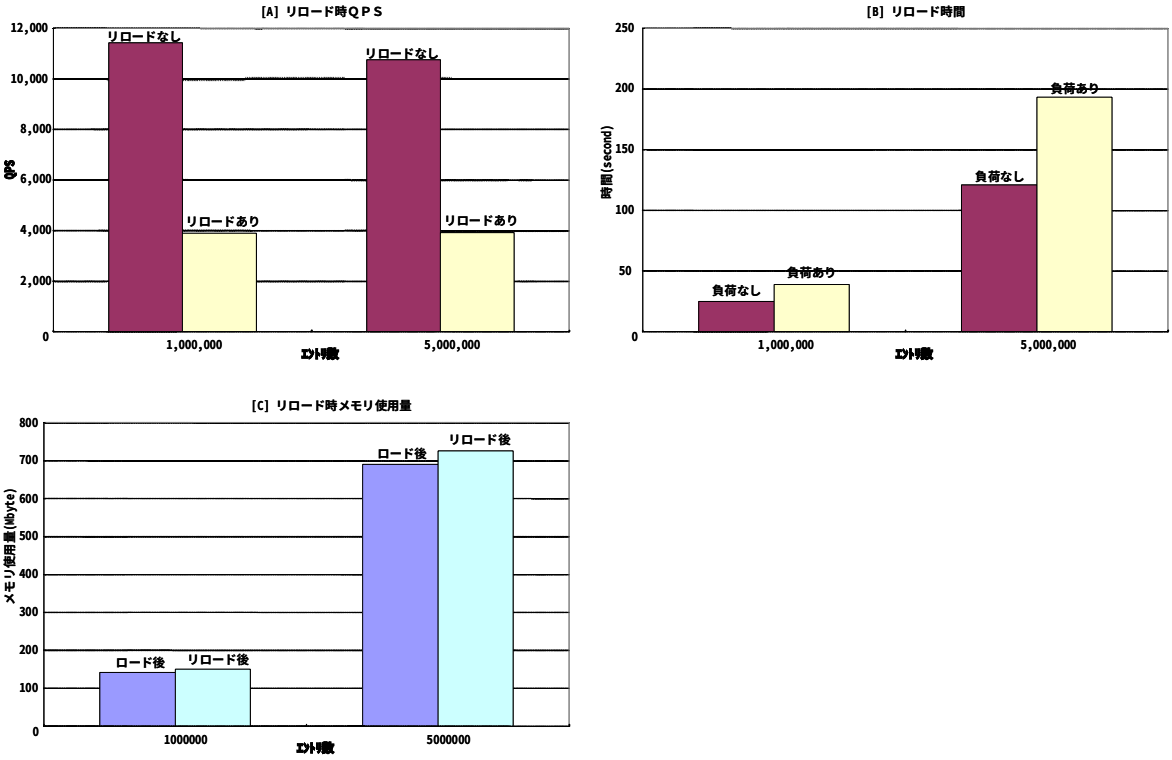


図 9 たけのこモデル Teir1 評価結果

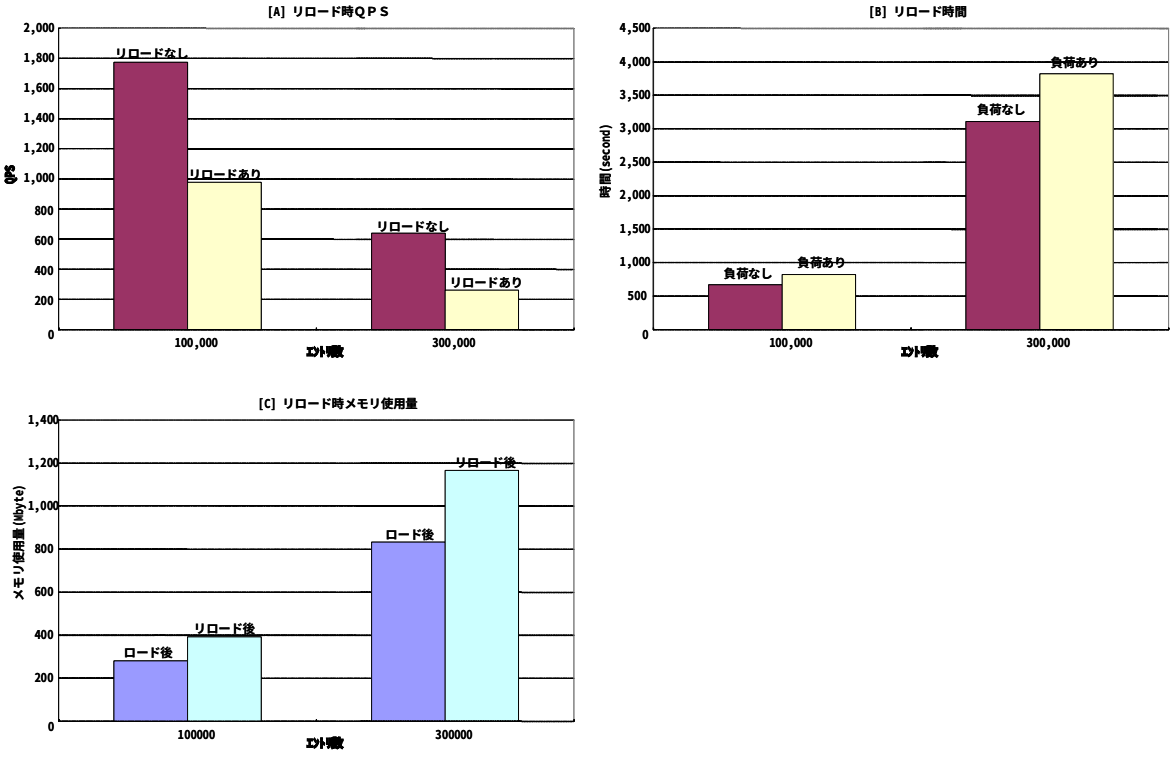


図 10 たけのこモデル Teir2 評価結果

3.1.2.7 今後の展開

今回、まだ評価を行っていない項目として、ENUM において DNSSEC を使用した運用モデルが挙げられる。ETJP の別ワーキンググループ PandS WG の報告書で論じられているように、セキュリティの観点からは、ENUM 運用において DNSSEC を用いることが推奨されている。

このことを現在の DNS 標準の観点より検討すると、

(1)サーバに保持されるデータ量の増加
(2)ゾーン署名時間の純増
(3)DNSSEC 署名鍵の更新問題
(4)NSEC レコード由来のゾーン情報の網羅的検索

などが発生することになる。

特に、上記(1)(2)については今回評価したパフォーマンス要件に対する直接のインパクトを発生し、(3)(4)については運用上のモデル検討などが必要となると考えられるため、DNSSEC 方式については、本 WG においても当初より考慮していた通り、引き続き検討を進めるべきであろう。

DNS WG においては、IETF において議論中の DNSSEC 標準化状況を鑑みつつ、PandS など他グループとの連携を深めることなどにより、上記(3)(4)の問題をも検討項目に加えながら、より統合的な DNS 運用スキーマの検討に向かうことを検討している。

3.2 会員の活動

3.2.1 株式会社アステック

「ENUM システムにおけるネットワーク解析」について、報告する。

3.2.1.1 ASTEC Eyes on the net の ENUM システムへの対応状況

ASTEC Eyes on the net（以下、ASTEC Eyes と表記）は、株式会社アステックが開発しているソフトウェアのネットワークアナライザである。ASTEC Eyes の ENUM 関連のデータへ

の対応状況は以下のとおりである。

- ENUM 関連データへの対応
  DNS の NAPTR レコード
- DNSSEC 関連への対応
  DS、DNSKEY、RRSIG、NSEC、OPT レコード
- ENUM サービスプロトコルへの対応
  SIP、H323、HTTP、SMTP など

3.2.1.2　ENUM システムにおけるネットワーク解析

3.2.1.2.1　ENUM システムのデータの流れ

ENUM システム全体のデータの流れを図 11 のように分類する。

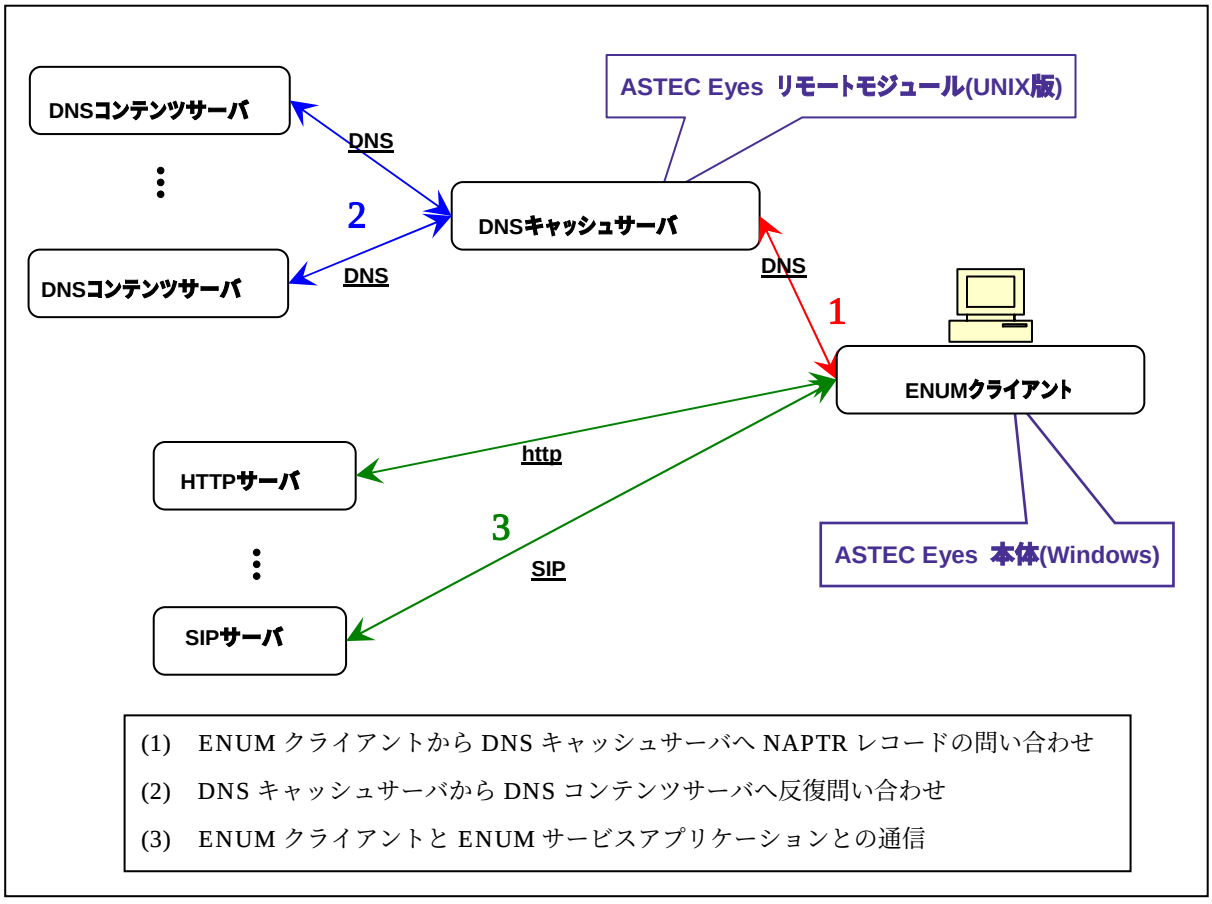


図 11 ENUM システムのデータの流れ

ENUM クライアント側にネットワークアナライザを置いた場合は、(1)と(3)に関するデータを

監視することができる。また、DNS キャッシュサーバ側にネットワークアナライザを置いた場合は(1)と(2)に関するデータを監視することができる。

3.2.1.2.2　リモートモジュール

ASTEC Eyes のリモートモジュールはネットワークからデータを収集する機能をもったエージェントとして動作し、リモートモジュールが取得したデータを ASTEC Eyes 本体で見ることができる。リモートモジュールは Windows 版の他に、Solaris 版、Linux 版、FreeBSD 版があるので、DNS サーバが UNIX 系の OS で運用されている場合でも直接インストールしてネットワークを監視することができる。

3.2.1.2.3　解析結果

3.2.1.2.3.1　ENUM 関連のデータの解析結果

ASTEC Eyes で NAPTR レコードを解析した結果（図 12）、および DS レコードと RRSIG レコードを解析した結果（図 13）を示す。

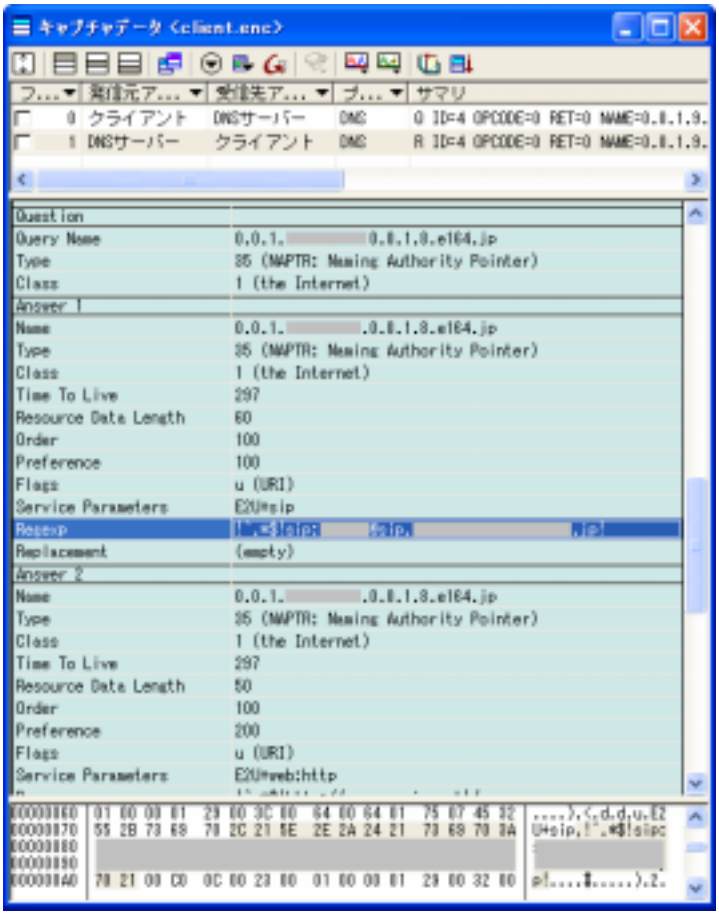


図 12　NAPTR レコードの解析結果

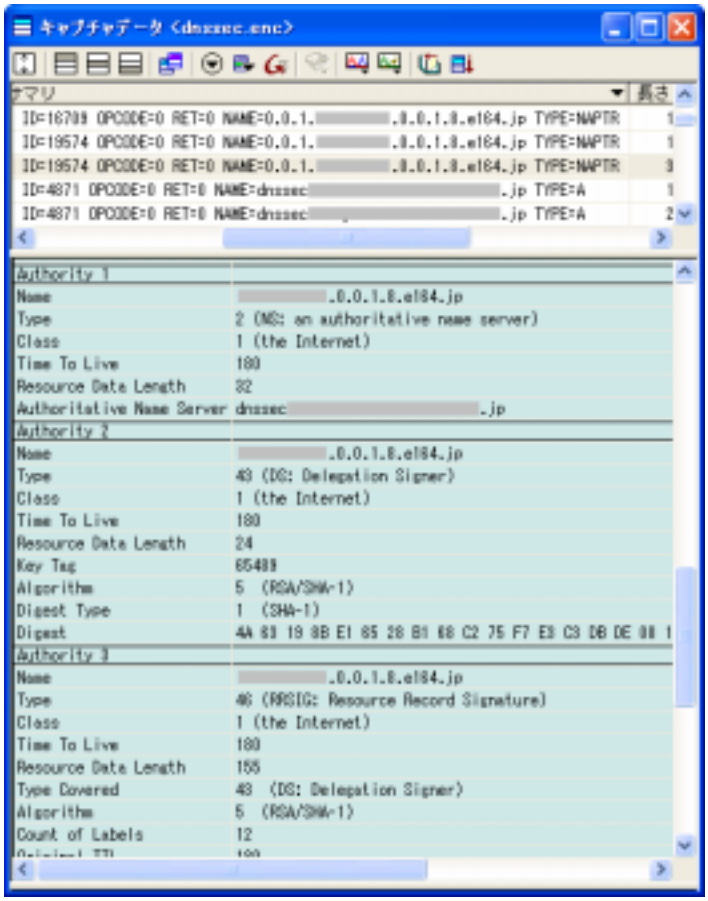


図 13　DS、RRSIG レコードの解析結果

3.2.1.2.3.2　DNSSEC データの解析結果

DNS キャッシュサーバ側でパケットをキャプチャして解析し、DNSSEC 関連のデータだけに絞り込んだ結果を示す（図 14）。このデータから DNS キャッシュサーバと DNS コンテンツサーバとの間で署名（RRSIG レコード）を伴ったデータの流れや、鍵の問い合わせ（DNSKEY レコード）の様子やタイミングなどを確認できる（図 15）。

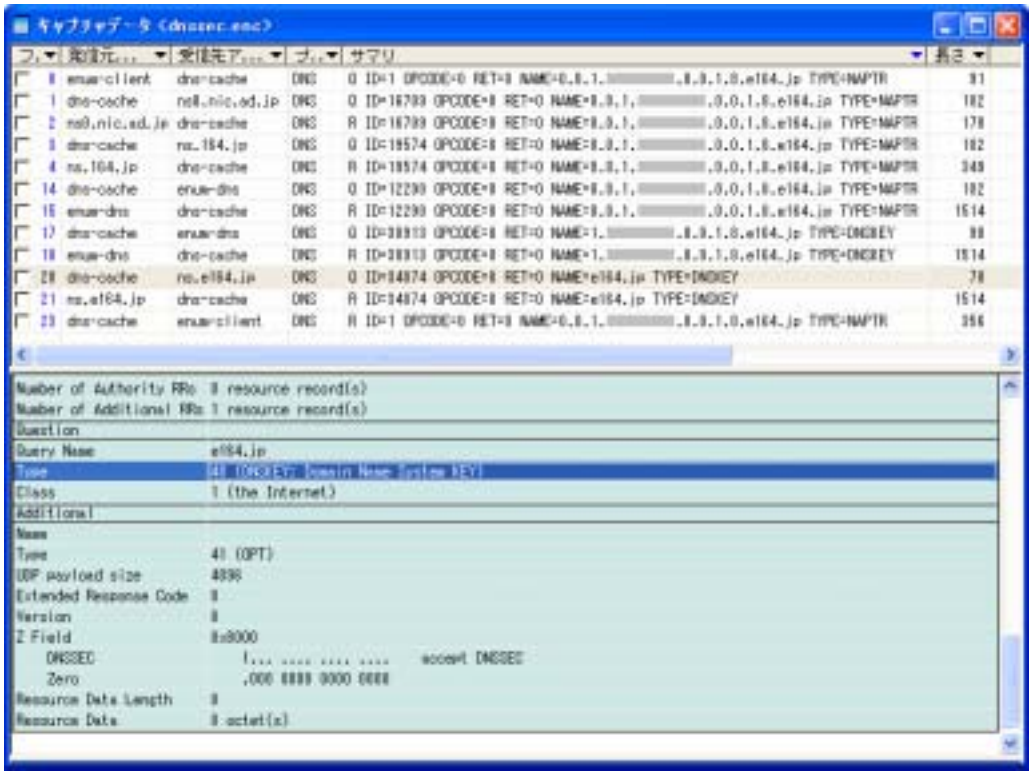


図 14　DNSSEC 関連のデータの解析結果

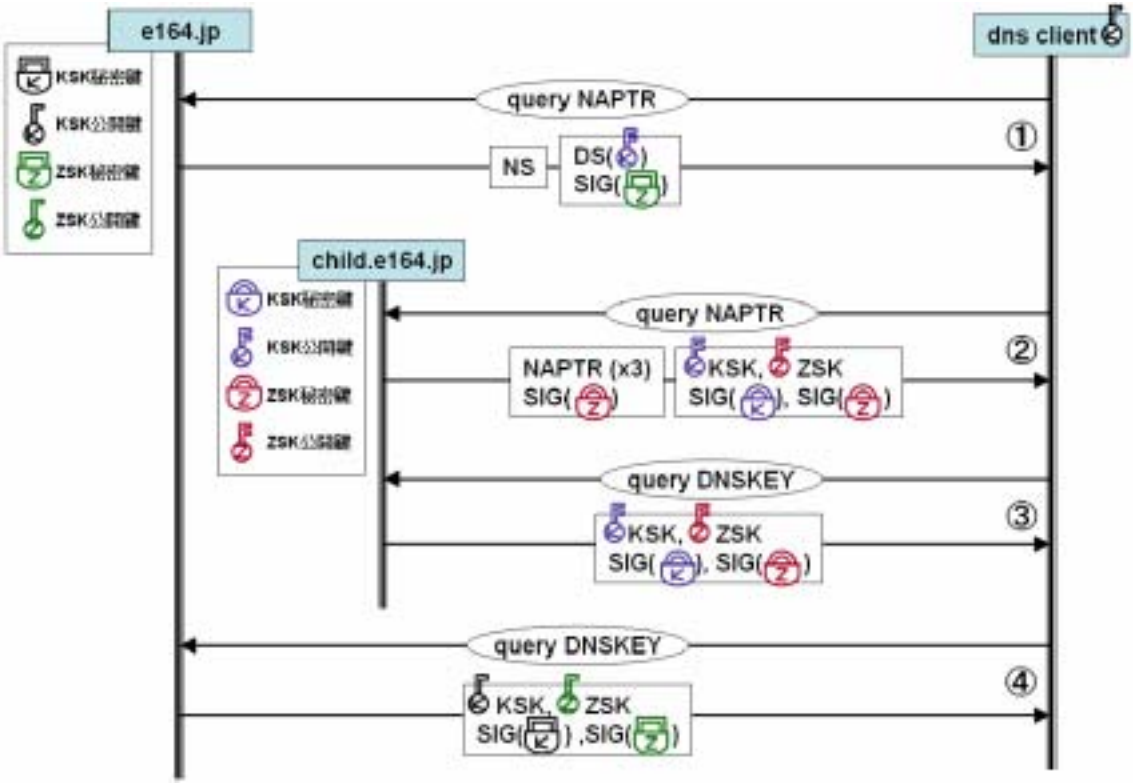


図 15　キャッシュサーバとコンテンツサーバの間のデータの流れ

3.2.1.2.4　IP パケットのフラグメント化について

DNSSEC に対応し、RRSIG レコードを含む DNS の UDP データはサイズが大きくなるため、IP レイヤでパケットのフラグメント化が発生する場合がある。この様な場合でも ASTEC Eyes は分割された 2 つ目以降のデータを自動で探し出し、結合して解析を行う（図 16）。
フラグメント化が発生するケースでは、パケットデータを取得する際に特定の UDP ポートに限定するようなフィルタをセットすると、分割された UDP パケットが取得できなくなるため注意が必要である。

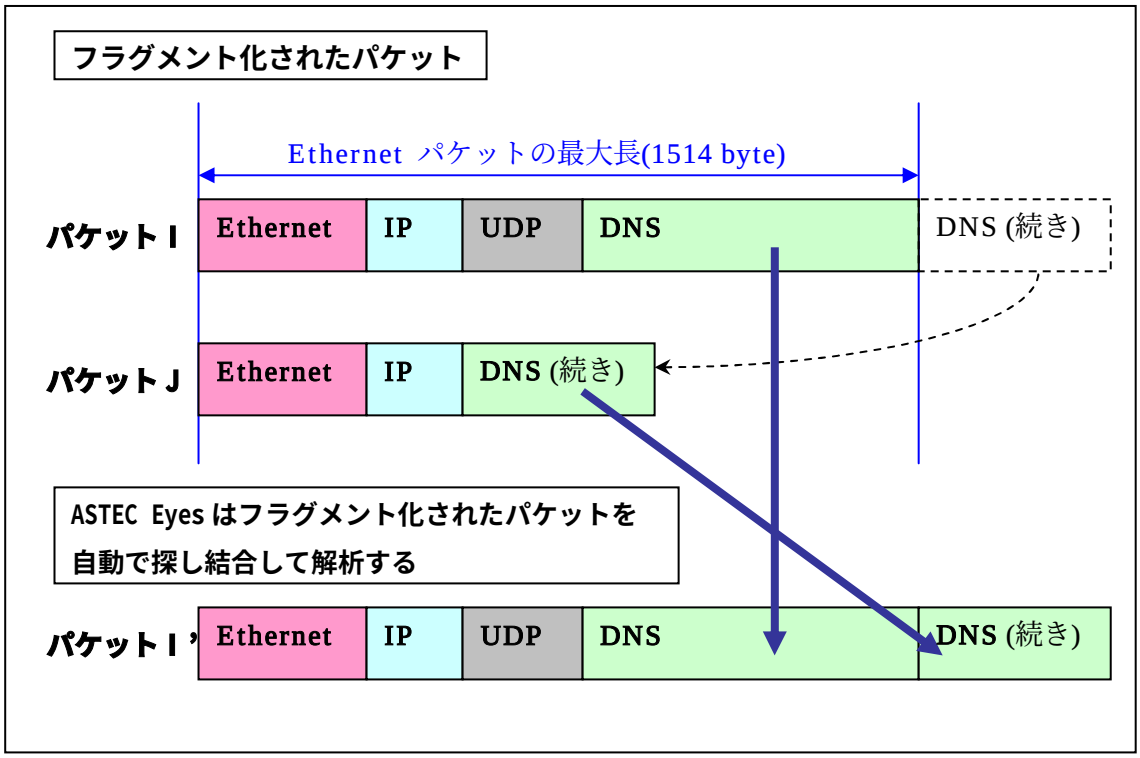


図 16　フラグメント化したパケットを結合して解析

3.2.2　日本テレコム株式会社

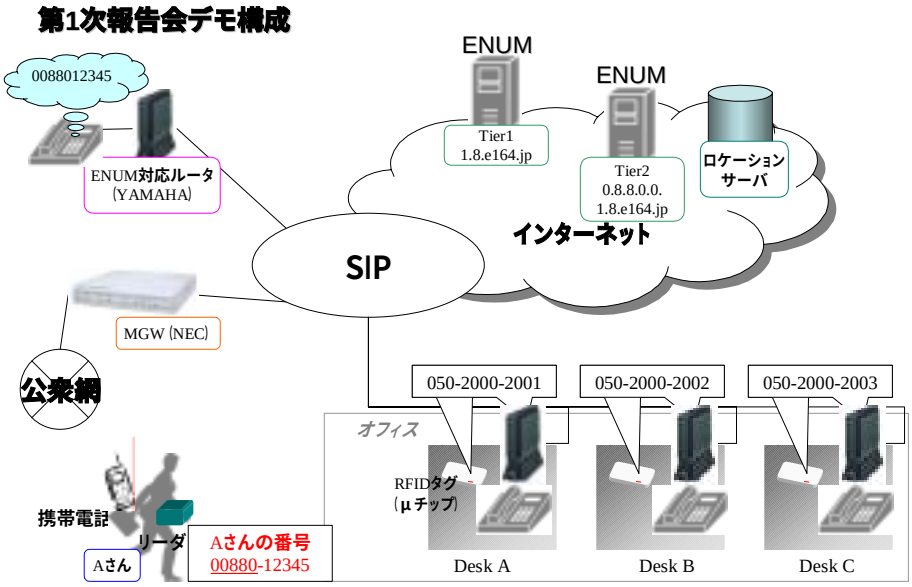
日本テレコムの ENUM に関する代表的な活動について報告する。

3.2.2.1　ETJP 第 1 次報告会におけるデモの紹介

日本テレコムでは、ENUM を使った新しいサービスを具現化することを目的とし、RFID と ENUM 技術を組み合わせた 1 ナンバーコールシステムの開発を行い、第 1 次報告会にて発表した。

このシステムは、電話を掛ける側が、掛けたい相手に付与された番号（ワンナンバー）をダイヤルすると、その人の位置や状況に応じて自動的に着信先を携帯電話や固定電話、IP 電話へ変更する仕組みを実現している。

例えば図のように第 1 次報告会におけるデモでは、電話をかける側が、掛けたい相手の番号「0088012345」をダイヤルすると、掛けたい相手が外出中の時は携帯電話へ着信し、会社のオフィスいれば携帯電話ではなく一番近くの電話に着信するように構成した。



図「ワンナンバーコールサービス with RFID」の概要

＜一連の動作概要＞

第 1 次報告会で行ったデモの動作概要を簡単に紹介する。

1. 外出中など、位置情報をロケーション DB が把握していない状況では、A さんのユーザ ID 番号に電話をかけると携帯などに着信するよう ENUM サーバーへあらかじめ設定

しておく。

例）ENUM サーバーにおける NAPTR レコード

5.4.3.2.1 IN NAPTR 100 10 "u" "E2U+SIP“ "!^.*$!sip:090……@……!"　.

2. この状態で 0088012345 とダイヤルすると、図の左上の ENUM 対応ルータは、ENUM サーバーに A さんの番号を問い合わせにいき、その結果、上記 NAPTR レコードが返ってくるので A さんの携帯電話に発信することとなる。
3. 次に、A さんがオフィスに入り、Desk A に着席する際、A さんの持つリーダで机（電話機）に貼り付けてある RFID タグを読み取る。
4. リーダは、そのタグの ID 情報を取得し、ロケーションサーバにユーザ ID やパスワード情報などと共に送信する。
5. ロケーションサーバは認証処理などを行ったあと、ユーザ ID とタグ ID と関連付けられた URI（電話番号情報）とを結びつけ、必要なデータを DB に収める
6. ロケーションサーバは、最新の状態に ENUM サーバーの zone ファイルを更新する。

例）ENUM サーバーにおける NAPTR レコード

5.4.3.2.1 IN NAPTR 50 10 "u" "E2U+SIP“ "!^.*$!sip:05020002001@……!"　.

5.4.3.2.1 IN NAPTR 100 10 "u" "E2U+SIP“ "!^.*$!sip:090…..@…..!"　.

7. 2.と同じ手順で A さんのユーザ ID に電話をかけると、ENUM 対応ルータは最新の zone ファイルを参照し、優先度の高い sip:05020002001@--------の方の URI を選択する。その結果、A さんの席にある電話に着信することとなる。

① Networld+Interop2004　Tokyo での紹介

本システムをＩＰｖ６化し、「ワンナンバーコールサービス with RFID」と題してプロトタイプを P2P ゾーンに出展した。

② ITU　TELECOM　ASIA2004 での紹介

本システムに関して、「自動認識型 1 ナンバーコールシステム」と題して日本パビリオンの日本テレコムブースにおいてパネル展示した。

③ その他

日本テレコムでは、ETJP 実験活動の一環として、独自で ENUM サーバーを立ち上げ、ETJP の運用する ENUM サーバーと接続し、基本動作の確認や運用ノウハウの蓄積に努めてきた。

さらに、ETJP 内のワーキンググループへも積極的に参加し、DNS ワーキンググループにおける ENUM サーバーの性能評価実験のデータ収集活動を行ってきた。

3.2.2.2　今後の予定

日本テレコムでは、今後も ENUM の普及を目指し、積極的に推進していく。

3.2.3　株式会社日本レジストリサービス

第 1 次報告以降の、JPRS の活動について報告する。

3.2.3.1　ENUM Client/SDK 開発

JPRS では、ENUM の動作を視覚的に確認しプロトコルの理解を深めると共に、ENUM 対応アプリケーションの開発を促進する目的で ENUM Client/SDK を開発し、ETJP 全体ミーティングの場を通じて ETJP 会員に限定配布を行ってきたが、所期の目的を達したこと、ライセンスの整理がついたことから、2005 年 8 月末に一般配布を開始した。ENUM Client/SDK の概要および配布物を以下に示す。

3.2.3.1.1　ENUM Client/SDK 概要

1. ENUM SDK
   - ENUM アプリケーションを作成するためのライブラリ
   - プラットフォームは Windows
   - 開発は VC++で、OCX(ランタイムライブラリ)を提供
2. ENUM Client
   - ENUM SDK を使用して作成した ENUM のサンプルクライアント
   - 開発は VC++で、実行形式を提供

3.2.3.1.2　配布物

1. ENUM Client (日本語版、英語版)
   - ENUM Client(バイナリ)
   - ENUM SDK のインストールは不要
   - 日本語版・英語版の違いはメッセージのみ
2. ENUM SDK (日本語版、英語版)
   - ENUM SDK ランタイムライブラリ(バイナリ)
   - ENUM SDK を使用するサンプルプログラムコード(VC++、VB)
   - 日本語版・英語版の違いはメッセージのみ

3. ENUM SDK / ENUM Client ソース(日本語版、英語版)
   - VC++ソースプログラム(群)
   - インストーラープロジェクト
   - 日本語版・英語版の違いはライセンスと API 仕様書のみ
     (ソース中のコメントはどちらも日本語)

3.2.3.1.3　配布元

これらは JPRS の Web サイトからダウンロード可能である。

ENUM Info by JPRS
http://jprs.co.jp/enum/

SoftwareLibraries
http://jprs.co.jp/enum/software/software.html

3.2.3.2　APEET

JPRS が参加している APEET(Asia Pacific ENUM Engineering Team)の概要と、2005 年 2 月に京都で開催される APRICOT2005 で APEET が実施する体験デモについて、第 6 回 ETJP 全体ミーティングで紹介した。

3.2.3.2.1　APEET 概要

APEET、AP 地域で ENUM トライアルの推進を図っている ccTLD (CNNIC、KRNIC、SGNIC、TWNIC、JPRS)が中核となり、 2004 年 7 月 19 日に発足した法人格は持たない任意組織である。

http://www.apenum.org/

APEET は、メンバー相互で ENUM/SIP に関する技術交流やトライアルの連携を図ること、AP 地域のインターネット利用者に ENUM/SIP の普及・浸透を図ること、その具体的な目標として APRICOT2005 で ENUM/SIP の体験デモを実施することを目的としており、専用の ENUM-like ツリー(apenum.org)の元で実施している。
このツリーで使用している番号は E.164 番号とは無関係であり、APEET メンバーの宣言にもとづいて採番されている。

3.2.3.2.2　APRICOT2005 での APEET による ENUM/SIP 体験デモ

ENUM/SIP 体験デモは、APRICOT2005 会場で会議参加者に SIP/ENUM を使ってもらい、ENUM/SIP の普及・浸透を図ることを目的としている。具体的な実施内容とイメージを図 17 に示す。

- APRICOT2005 参加者への APEET ENUM-Like ツリーの元での番号割当
- 会場内での無線 LAN 対応携帯電話型 SIP 端末の貸出・販売
- 当該端末、PC 用 SIP ソフトウェア、APEET デモブースでの設置機器等を利用した ENUM/SIP による相互通信
  + 会場内<-->会場内
  + 会場内<-->会場外

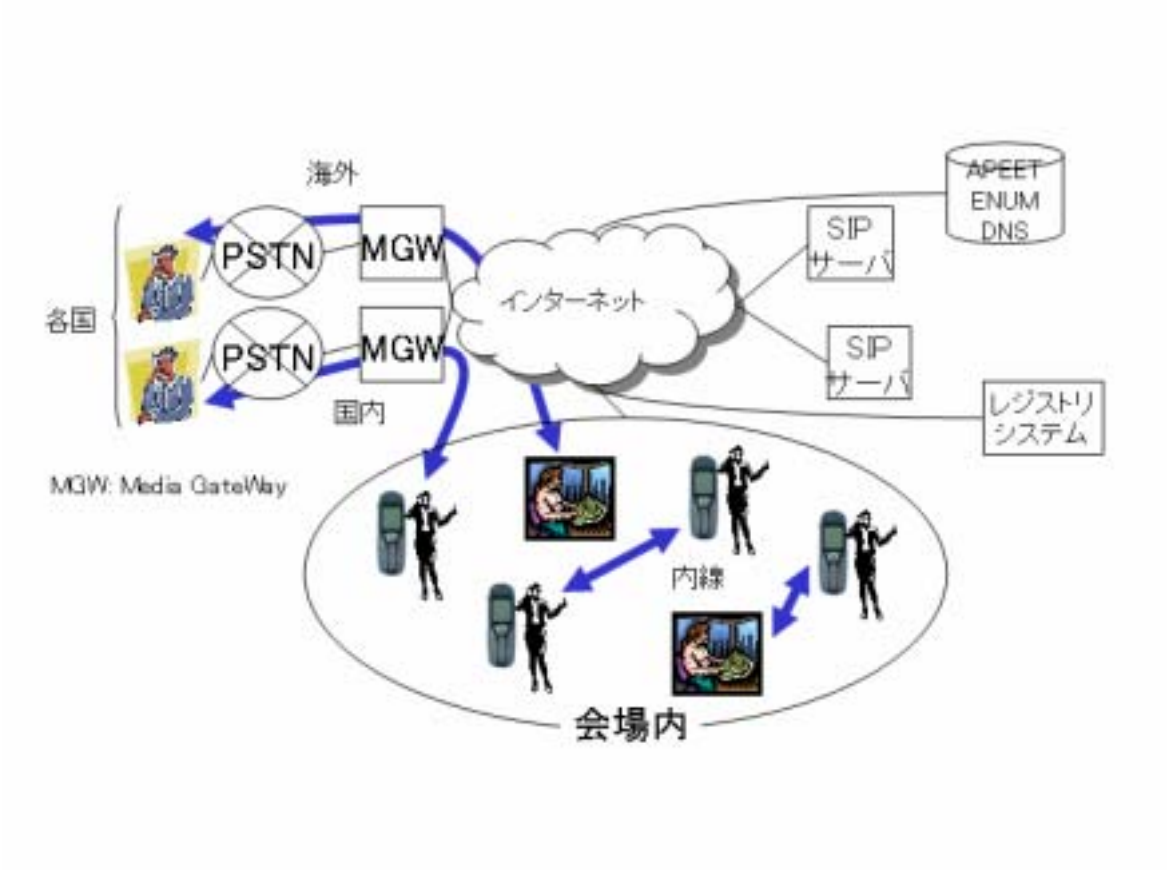


図 17　Live Demo イメージ

3.2.3.3 IETF

2004 年 8 月に行われた IETF 会議の概要と、JPRS の IETF での標準化活動報告を行った。

3.2.3.3.1 IETF San Diego enum WG 報告

2004 年 8 月 1 日から 6 日に San Diego にて IETF 会議が開催され、8 月 4 日に ENUM WG の会議が開催された。今回の会議では、2 時間の枠を半分に区切り、前半を通常のワーキンググループの打ち合わせ、後半をキャリア ENUM ミニ BoF として議論を行った。

前半では、主に 3 つのインターネットドラフトについて議論された。まず、VeriSign の Scott Hollenbeck 氏から ENUM でのレジストリ登録に関するプロトコル提案についての説明があった。この提案は 8 月下旬にワーキンググループで合意され、9 月 3 日に IESG に提出された。次に、JPRS の藤原から、ENUM を実装した結果判明したプロトコル上の問題を書いたインターネットドラフトの進捗状況を報告し、著者が Open Issue としてあげた部分について、著者の考えをまとめ、修正すればワーキンググループラストコールとすることとなった。この提案内容については後述する。最後に、オーストリアの Richard Stastny 氏から、キャリアがオペレータ ENUM を行う場合に、使っていない番号を表すための voidservice の提案があり、議論の結果、ワーキンググループで取り扱う項目として扱うこととなった。

後半のキャリア ENUM ミニ BoF では、様々な提案や議論が行われたが、議論がうまく進まず、結果として発散し、参加者に対してキャリア ENUM についての意識調査を行った結果、キャリア ENUM についての共通認識がないということが認識された。

3.2.3.3.2 JPRS の IETF での標準化活動

JPRS では昨年から ENUM クライアントの試作を行ってきているが、その過程で ENUM 関連 RFC に含まれる問題点を見つけた。その内容を 2004 年 3 月にソウルで開催された IETF 会議で報告したところ、重要な内容であるため、イギリスの Lawrence Conroy 氏が書かれた実装上の問題点をまとめたドラフトに今回の内容を追加し、ワーキンググループとして標準化を行うドキュメントとすることになった。2004 年 8 月の IETF 会議にまにあう形で Conroy 氏と藤原共著の形でドキュメントを提出し、IETF 会議にて、決めかねている点についての意見をもらい、10 月にほぼ最終形のドキュメントとして提出した。

> "ENUM Implementation Issues and Experiences",
> ENUM を実装した結果判明した問題点,
> Lawrence Conroy, Kazunori Fujiwara, 25-Oct-04,

<draft-ietf-enum-experiences-01.txt>

この中で、RFC には細かい内容が明記されていないことで、解釈の違いにより相互接続性に問題が生じる可能性あることについて、ENUM に期待されている機能を損なわずに、実用的なレベルでクライアントを実装可能とする要求条件や、注意点をまとめている。

4. 今後の予定

ETJP は、活動期間を当初 1 年間としていたが、2004 年 9 月にさらに 1 年間の延長をすることを決めた。延長の目的は、設立 1 年以内に通信事業者間のサービス実験や国際実験であるフェーズ 3 までを終了させることができなかったため、そのフェーズを終了させるためである。
フェーズ 3 を終了させるためには、ENUM トライアルのドメイン、”1.8.e164.arpa”が必要と考えられているが、ETJP は、関連機関と共にその委任に深く関わっていくこととする。
また、フェーズ 1、フェーズ 2 においても引続き、広くにわたって実証実験を進めていく。
さらに、IP 電話技術の関連団体とも協力を進め、ENUM 及び ENUM を使ったアプリケーションやサービスの実証実験に貢献していきたい。