

権威DNSサーバの デュアルスタック化による問題と その報告

dnsops.jp BoF
Internet Week 2008

民田雅人
株式会社日本レジストリサービス

JP DNSサーバの構成について

- 2008年10月版 -

<<http://jprs.jp/tech/jp-dns-info/2008-10-06-jp-dns-servers.html>>

▼IPv4だけのDNSサーバについて

<中略>

JP DNSなどの**権威サーバですべてのDNSサーバがIPv4/IPv6のデュアルスタックになると**、キャッシュサーバの実装とそのネットワーク環境によっては**不具合がおきることがある**という報告があります。これについての**詳細は未確認**ですが、JP DNSでは、運用面の安全性を考慮し当面の間IPv4だけのサーバを維持する方針で運用するため、新たにg.dns.jpをIPv4のみのサーバとして追加します。

「不具合がおきることがある」とは？

- Ed Lewisさんの「j.gtld.biz's A record is missing!」
dnsops.jp BoF@Internet Week 2007
 - この質疑応答の中でちらっと出てきた話
- 後からEd Lewisさんに聞いてみた
 - 「ちょっと前のBIND 9だと、IPv6の接続性がよくないときにうまく検索できないみたいだから1個だけでもIPv4だけのサーバを残しとくのがオススメ」
 - 「BIND 9では2004年1月ぐらいに直ったよ」

「詳細は未確認」のままではいけない

- 実は1度調査したが、結果がいまひとつ
 - 仕方なく「詳細は未確認」と表記
 - 理由は、十分なDNSのテスト環境を構成しきれなかった

テスト環境作るのめんちゃいなあ...

作ったとして再現できるのかなあ...



漢だね .INFO !

- .infoは全部IPv4/IPv6 Dual Stack
 - ある日root zoneを眺めていて気づく
- ということは...
 - .jpの適当なドメイン名と .infoの適当なドメイン名をキャッシュサーバに検索させて比較すればOK!
 - .jpにはIPv4 onlyあり



調査方法

- 調査専用の環境(OSとネットワーク)を用意
- IPv6対応のBINDを一式コンパイル
- キャッシュサーバを起動し、.jpと.infoのドメイン名を検索させ、検索にかかる時間をtimeコマンドで計測
- TLDのNSとGlueがキャッシュにある場合と無い場合を調べるため、それぞれのTLDで2種類のドメイン名を対象にする
- 他のドメイン名の影響をうけたくないので、ネームサーバが**内部名**のドメイン名を選ぶ
 - ドメイン名 example.jp
 - ネームサーバ名 XXXX.example.jp

調査ドメイン名の候補選び

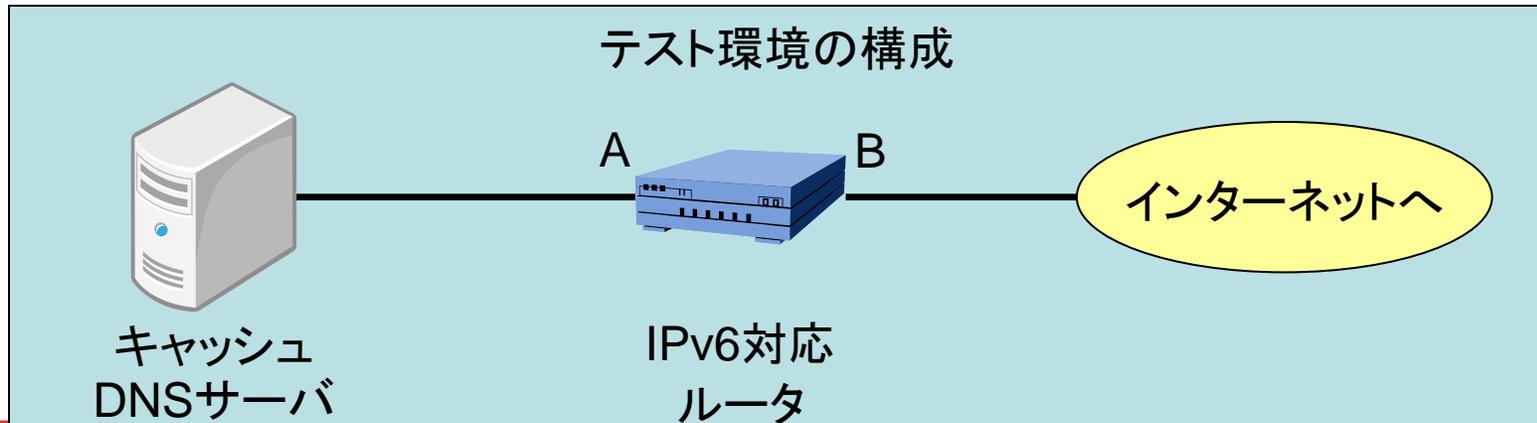
- 内部名なのを2つ .jpは簡単、でも .infoが...
 - どーしてみんな、NSは.comとか.netとかetc. ...
- ふと、知人の .infoドメイン名を思い出す
 - 調べたら内部名だった
 - でもFLET'S ISDN(64kbps)の先に
ネームサーバがあるんですけど...
- 念のため本人に許可を頂く
 - ゆっくり(2~5クエリ/sec程度?)だけど1万クエリ以上!
- 快諾を得て調査開始



Thankyou

用意したネットワーク環境

- IPv6の接続性がだめな場合って何？
- パターンA: サーバのIPv6はLinklocalアドレスのみ
 - IPv6対応OSを使った場合にありがちな環境
- パターンB: サーバにグローバルなIPv6アドレスはあるが、接続性が無い
 - ルータのA側のみにIPv6アドレスをつけ、RAを送出する

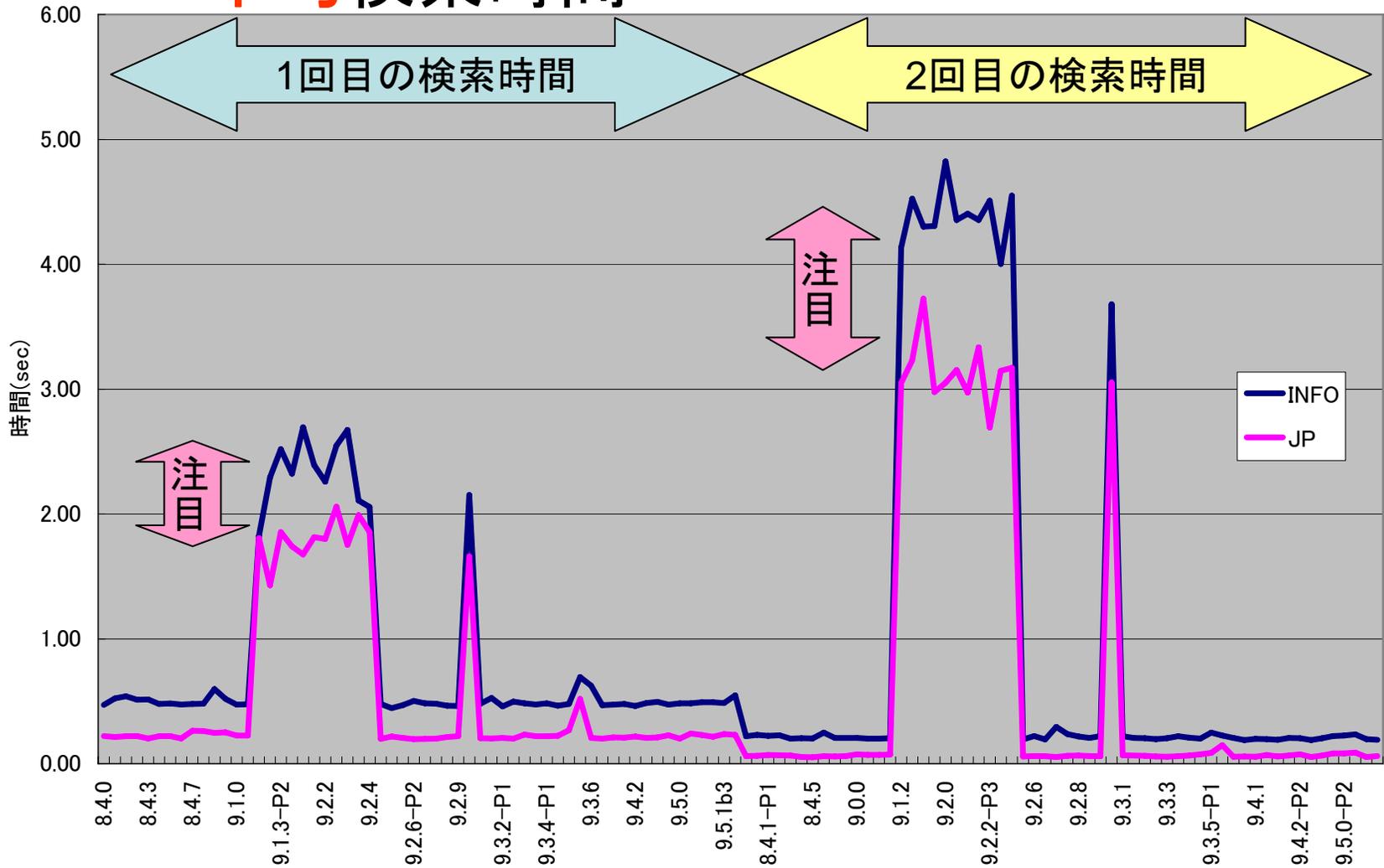


テスト方法

1. キャッシュDNSサーバプログラムを起動
 2. ドメイン名1を検索し時間を計測
 - TLDのNSレコードとGlueをキャッシュする
 3. 同じTLD内のドメイン名2を検索し、時間を計測
 4. DNSサーバプログラムを停止
- 1～4を同じ対象(BIND 58バージョンとTLDの組)で100回繰り返す、ドメイン名1、ドメイン名2でそれぞれ集計
 - パターンAは100回実行できたが、パターンBは実装によっては膨大な時間がかかるので10回に短縮

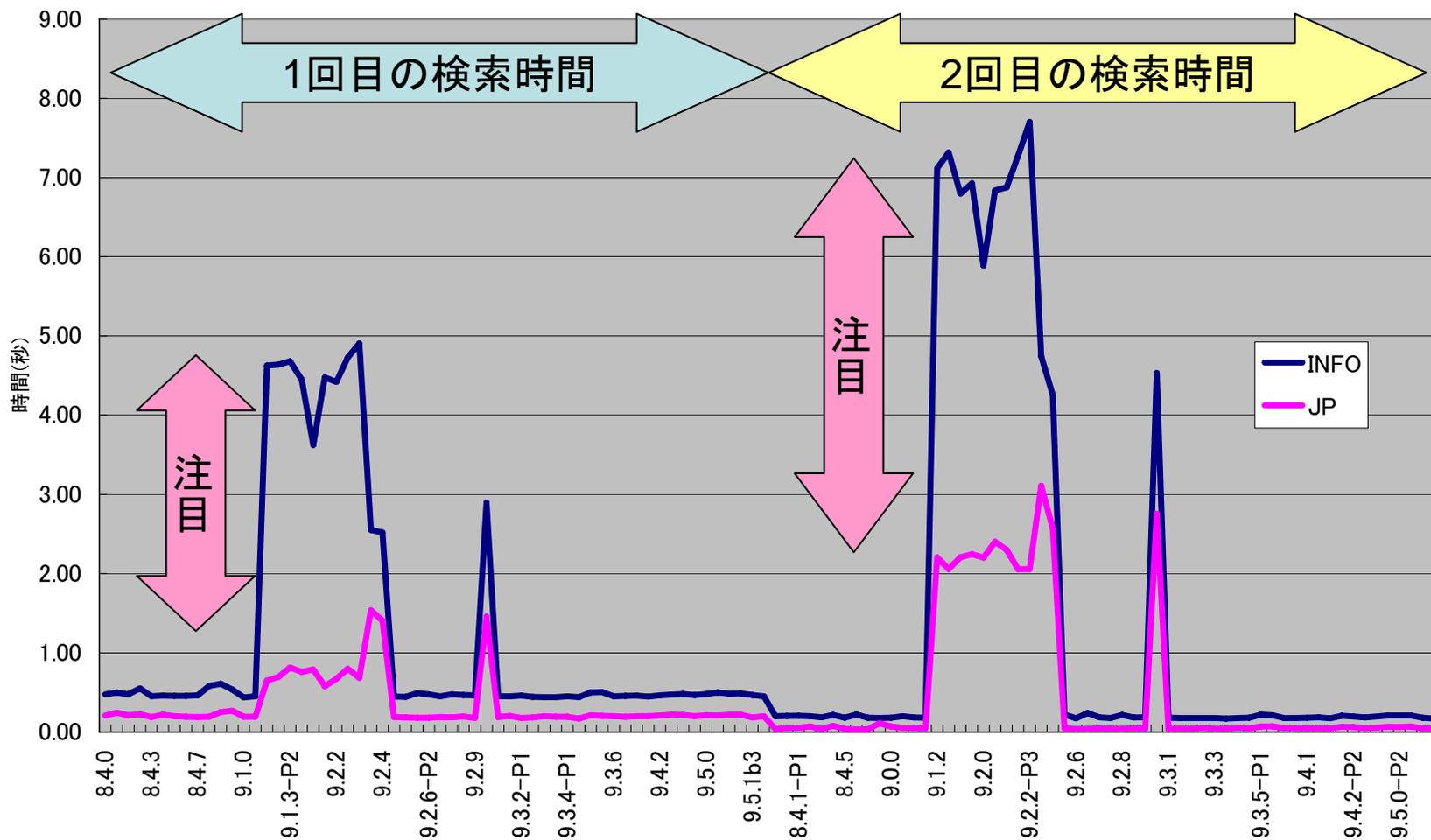
IPv6アドレスがLinklocalのみ

平均検索時間



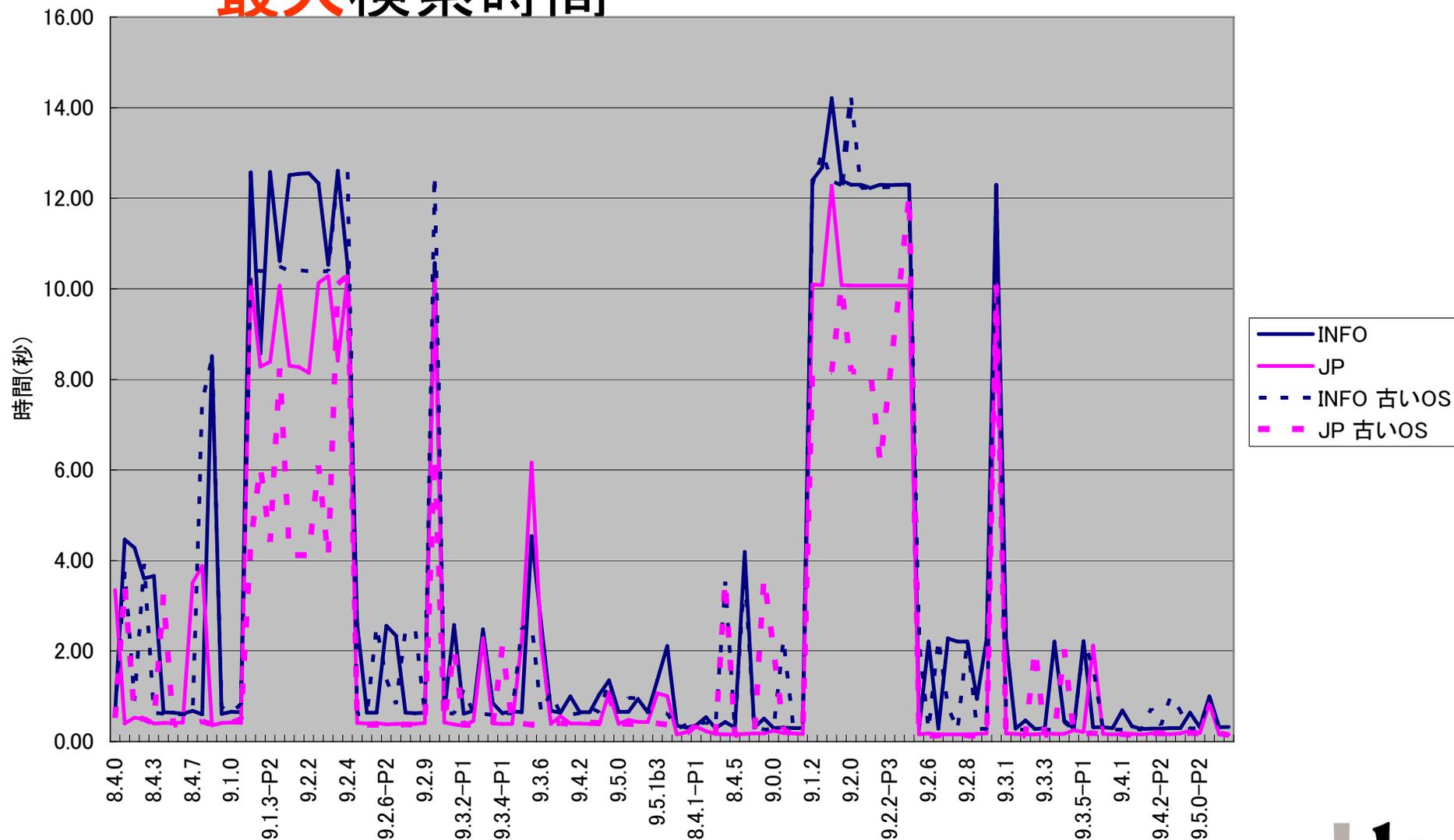
IPv6アドレスがLinklocalのみ(古いOS)

平均検索時間



IPv6アドレスがLinklocalのみ

最大検索時間

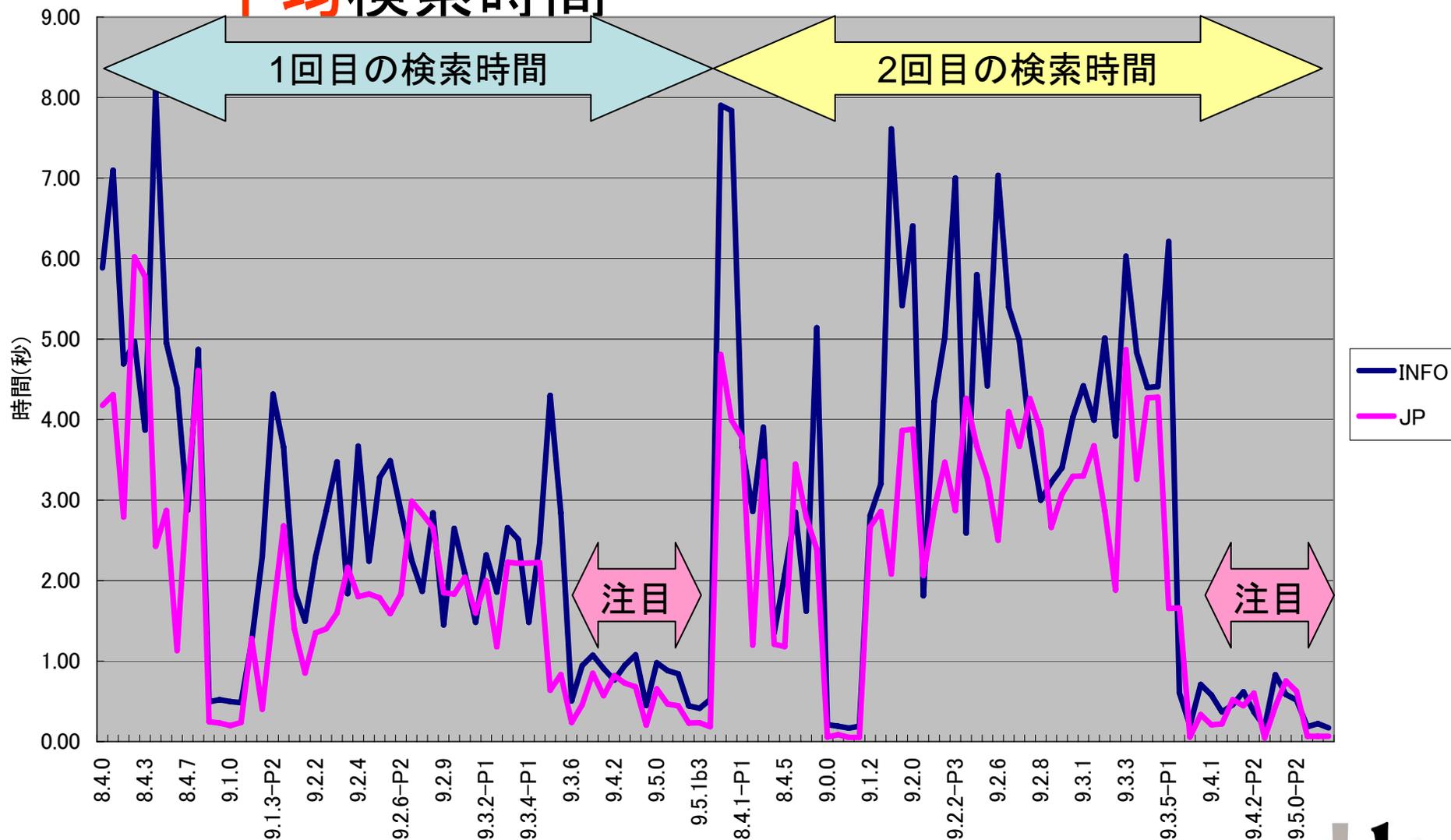


IPv6がLinklocalだけの場合

- 検索に時間がかかるBIND 9.1.2～9.2.4, 9.3.0
 - これらは、IPv6アドレスを持つNSがあるだけで検索時間が延びるようになる
 - 権威サーバがすべてDual-Stackだと、IPv4だけの権威サーバがある場合に比べさらに検索に時間がかかる
 - OSの実装によっては、すべてDual-Stackの場合の検索時間が極端に延びることがある
 - 現在利用することは推奨できないバージョン
- いずれのBINDでも、検索不能という致命的状態は発生しない

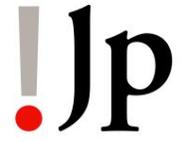
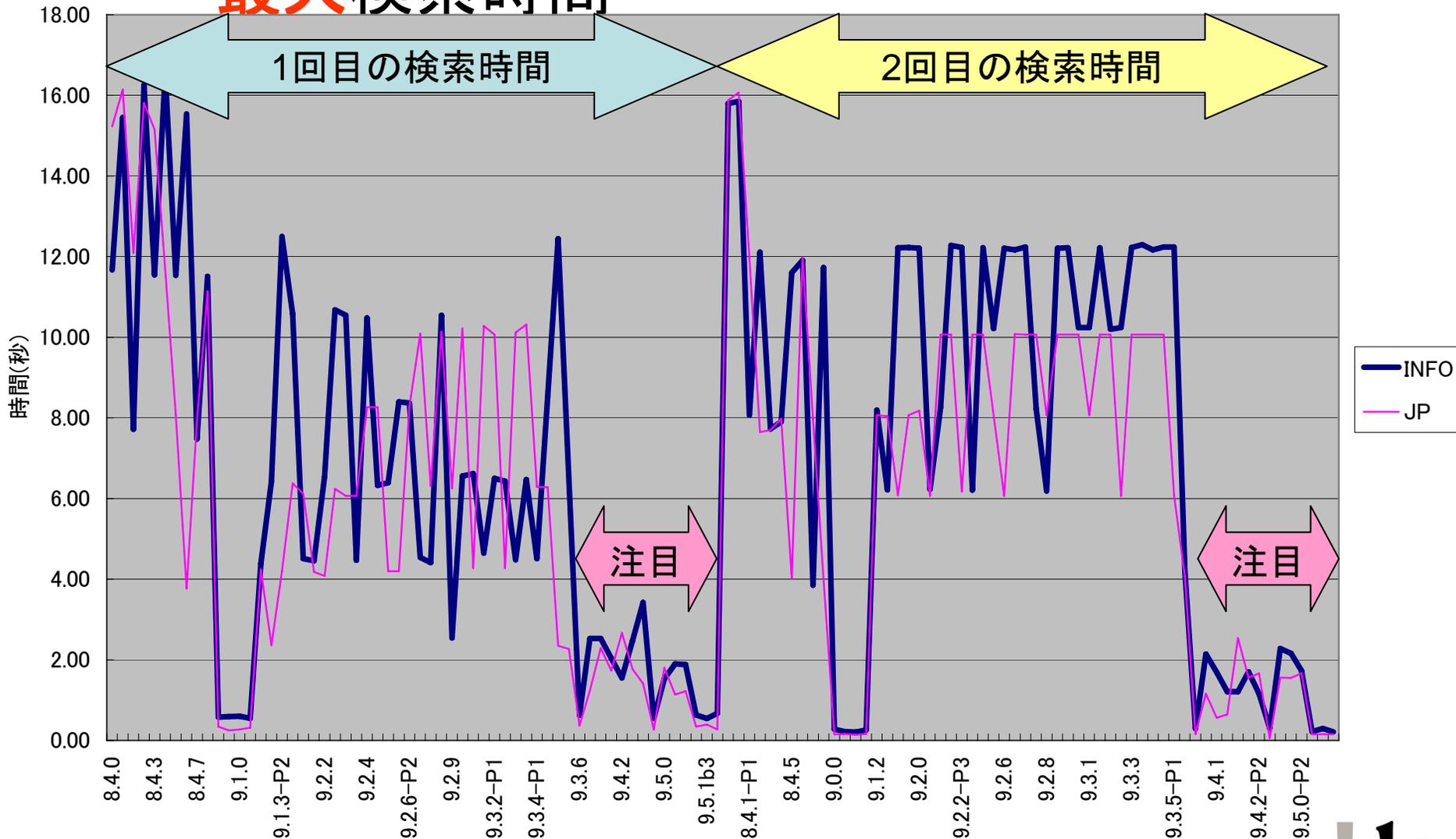
IPv6アドレスがあって接続性がない場合

平均検索時間



IPv6アドレスがあって接続性が無い場合

最大検索時間



IPv6アドレスがあっても接続性が無い

- OSの違い、権威サーバが全部Dual-Stackか、一部にIPv4があるかについての顕著な差は無い
- いずれのBINDでも、検索不能という致命的状態は発生しない
- 特に、BIND 9.3.6, 9.4.3, 9.5.1(b), 9.6.0(b)はIPv6の接続性が無くても、検索時間にほとんど影響しない

BINDではない実装は？

- UnboundとPowerDNS Recursorを調査
 - Unboundは1.1.1、pdns_recursorは3.1.7
- 権威サーバが全部Dual-Stackかそうでないかで、差はほとんど見られない
 - Linklocalだけの場合は、いずれも問題は発生しない
 - IPv6の接続性が無い場合、pdns_recursorは、最新のBINDと同程度。Unboundはやや時間がかかる(1回目の検索は1秒を少々超える程度)が実用範囲

まとめ

- 権威サーバがすべてIPv4/IPv6のDual-Stackになると、BINDの一部では、ドメイン名の検索に時間がかかるようになる。
 - ただし該当するBINDのバージョンは、現在は使用するのは推奨できないもの
- 新しいBINDや、最近の実装であるPowerDNS RecursorやUnboundは、そのような環境でも問題が発生しない

協力: 古場正行氏

Q and A

