BIND9の最新動向

株式会社日本レジストリサービス
坂口　智哉

目次

1. BIND9.9の主な新機能と変更点
2. バージョンアップ時の応答内容の比較
3. ゾーン転送中のクエリ処理性能

注意事項

- 本資料の機能は、執筆時点の最新リリース（BIND9.9.1-P2）を前提としたものです
- 本資料に登場する性能評価は、あくまでJPRS内で用意したテスト環境における結果であり参考値です
- 決して、開発元（ISC）のまわし者ではございません
  - 皆様のDNSの運用にお役立てできれば幸いです

1．BIND9.9の主な新機能と変更点

BIND 9.9の主な新機能・変更点 ＜権威DNSサーバー編＞

- ✓複数ゾーンの読み込み時間を短縮
- ✓デフォルトのゾーンファイルフォーマット変更
- ✓also-notifyオプションの構文拡張

複数ゾーンの読み込み時間を短縮

- BIND 9.8までは、複数のゾーンの読み込みに時間がかかっていた
  - ゾーンを管理するタスクの数が8個に固定されていたため
- BIND 9.9では、タスクの数をゾーンの数に応じて動的に変更
- ゾーンの**読み込み時間が短縮**
  - 条件によっては、2%程度のメモリ消費量の増加と引き換えに**読み込みが3倍～20倍高速化**

デフォルトのゾーンファイル フォーマット変更（1）

- スレーブ（ゾーン転送を受けるDNSサーバー）が書き出すゾーンファイルのデフォルトフォーマットが「raw」に変更
- BIND 9.8系までのデフォルトは「text」
  - RFC 1035などでフォーマットが定義されているもの
- 起動時の**ゾーンの読み込み時間が短縮**

- 「raw」は内部構造を表現したバイナリフォーマット
  - 人間が直感的に読めるものではない

デフォルトのゾーンファイル フォーマット変更(2)

- 従来の「text」フォーマットが必要な場合
  - 設定で、**従来のtextフォーマットで書き出す**こともできる

```
options { masterfile-format text; };
```

  - BIND 9に付属のnamed-compilezoneコマンドで、text形式に変換することもできる

```
$ named-compilezone -F text -f raw ¥
-o（出力ファイル名）（ゾーン名）（ゾーンファイル名）
```

also-notifyオプションの構文拡張（1）

- スレーブゾーンのalso-notify

```
zone ”example.jp” {
        type slave;                          ①
        also-notify [port ip_port] {
                ( masters_list | ②
                ip_addr [port ip_port] [key key] );
        };                                          ③
}
```

① ポート番号をまとめて指定できるようになった
② NOTIFYを送る先を、mastersで定義したリストで指定できるようになった
③ NOTIFY専用のTSIG鍵を指定できるようになった

also-notifyオプションの構文拡張(2)

- NOTIFY専用のTSIG鍵
  - 同じ名前のゾーンを、複数のビューに別々の内容で持たせるとき、それぞれにTSIG鍵を指定する
  - **特定のビューにあるゾーンにのみ、NOTIFYを送信**できるようになる

- 構文の拡張は後方互換性のある形で行われている
  - BIND9.8以前からBIND9.9へのバージョンアップ後でも、**以前のalso-notifyオプションの記述をそのまま利用可能**

BIND 9.9の主な新機能・変更点 ＜キャッシュDNSサーバー編＞

- ✓NXDOMAINのリダイレクト機能
- ✓RFC 1918の逆引きゾーンがビルトイン化

NXDOMAINのリダイレクト機能

- NXDOMAIN（該当するドメイン名なし）になる応答を特定のIPアドレスにリダイレクトする
  - 例えば、キャッシュDNSサーバーの利用者がタイプミスなどで**存在しないドメイン名を問い合わせた際、検索サイトなどにリダイレクト**させることが可能
  - 設定例については、ソースパッケージに同梱されているREDIRECT-NOTESを参照

- ただし、
  - ゾーンが**DNSSECで署名**されている
  - クライアントが**DNSSEC検証結果を要求**（DO bit ON）

  の両方を満たす場合には、**リダイレクトは行われない**

RFC 1918の逆引きゾーンがビルトイン化

- RFC 1918で定義されているプライベートIPの逆引きゾーン全てが、ビルトインのゾーンとして追加
  - RFC 6303の発行に基づく変更
  - プライベートIPアドレスの逆引きゾーンの定義で、空のゾーンとなっているためNXDOMAINを返す
  - 本来インターネットに出てはいけない**不適切なDNSクエリーを減らせる**

- named.confでゾーンを定義することで上書きできる
  - これまでどおり、プライベートIPアドレスの逆引きを設定することができる

BIND 9.9の新機能・変更点 ＜DNSSEC編＞

- ✓インラインDNSSEC署名
- ✓dnssec-signzoneの機能拡張

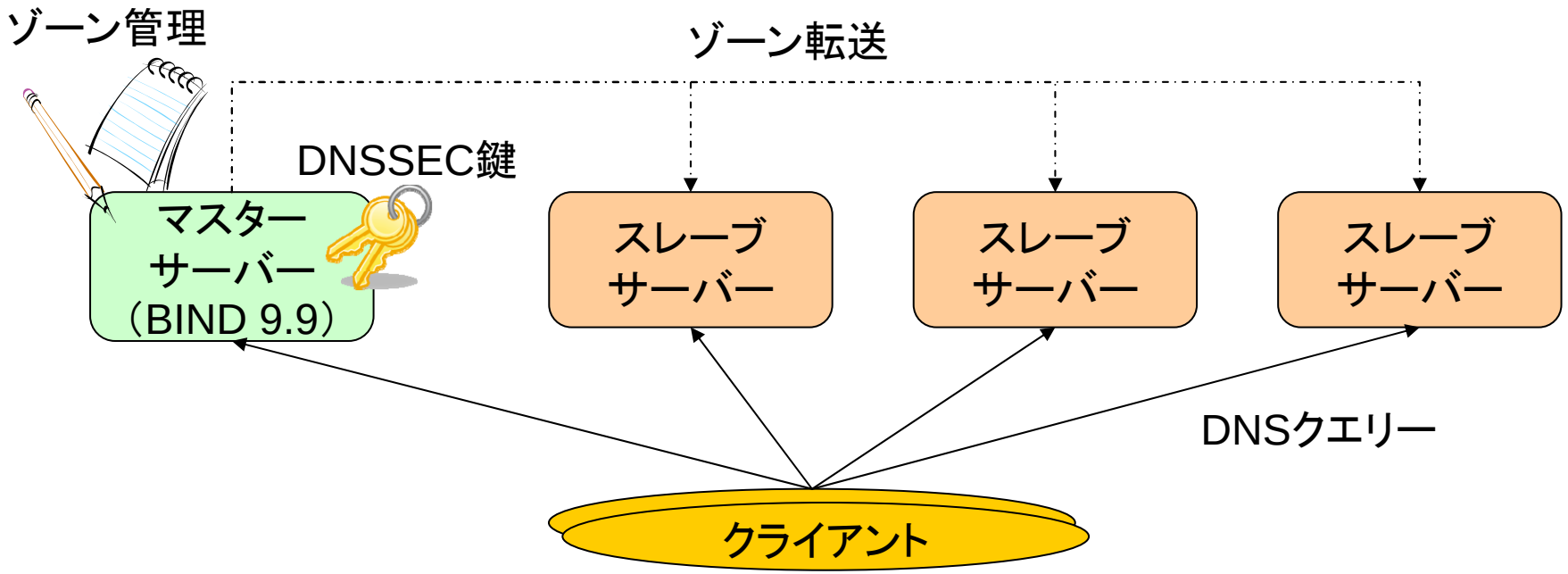
インラインDNSSEC署名（1）
概要

- ゾーンのマスター内やマスターとスレーブの間で、DNSSEC署名を自動的に行う
  - DNSクエリーを受け取ったタイミングで署名を行って応答する機能（ダイナミックDNSSEC署名）ではない

- これまでのゾーンの更新手順を変更することなく、透過的にDNSSEC署名を行える
  - dnssec-signzoneを手動で実行する必要はない
  - 署名前のゾーンが更新されたことを検知すると、namedが自動的に署名済みのゾーンを更新する

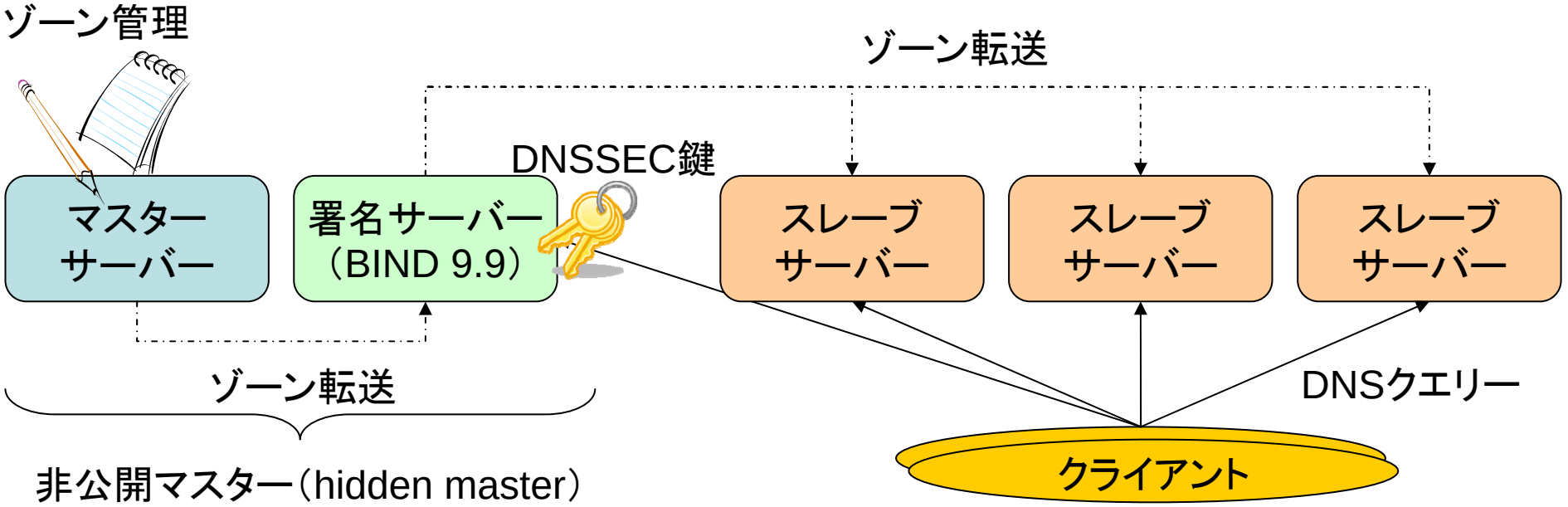
＜参考＞
https://kb.isc.org/article/AA-00626/0/Inline-Signing-in-ISC-BIND-9.9.0-Examples.html

インラインDNSSEC署名（2）
導入例1: マスターサーバーで署名



- マスターサーバーでDNSSECの鍵ペアを作成
- マスターサーバーでインライン署名の設定を追加
- ゾーン更新時に自動的に署名し、署名済みゾーンを読み込み
- スレーブには署名済みゾーンを転送
- SOAレコードのシリアル値はオリジナルのゾーンとは違うものになる

インラインDNSSEC署名（3）
導入例2: 署名サーバー追加



- 既存の構成に、署名サーバーを追加
- ゾーンを管理するマスターサーバーから署名サーバーへゾーン転送
- 署名サーバーでは自動的に署名を行い、署名済みゾーンをスレーブへ転送
- マスターサーバー、スレーブサーバーはBIND 9でなくても利用可能

※非公開マスター (Hidden Master)構成が前提

dnssec-signzoneの機能拡張

- dnssec-signzoneコマンドとは
  - ゾーンにDNSSEC署名を行うBIND 9付属ツール

- 下記オプションが追加
  - DNSSEC関連のレコードを別ファイルに保存 (-D)
    - $INCLUDEでインクルードできる形となる
    - オリジナルのゾーンファイルに変更を加えない
  - 存在しない鍵による署名を消去する (-R)
  - DNSKEY RRに対応するRRSIGの有効期限を変える (-X)
    - 普段はKSKの秘密鍵をオフラインにしている場合に便利

BIND 9.9の新機能・変更点 ＜その他＞

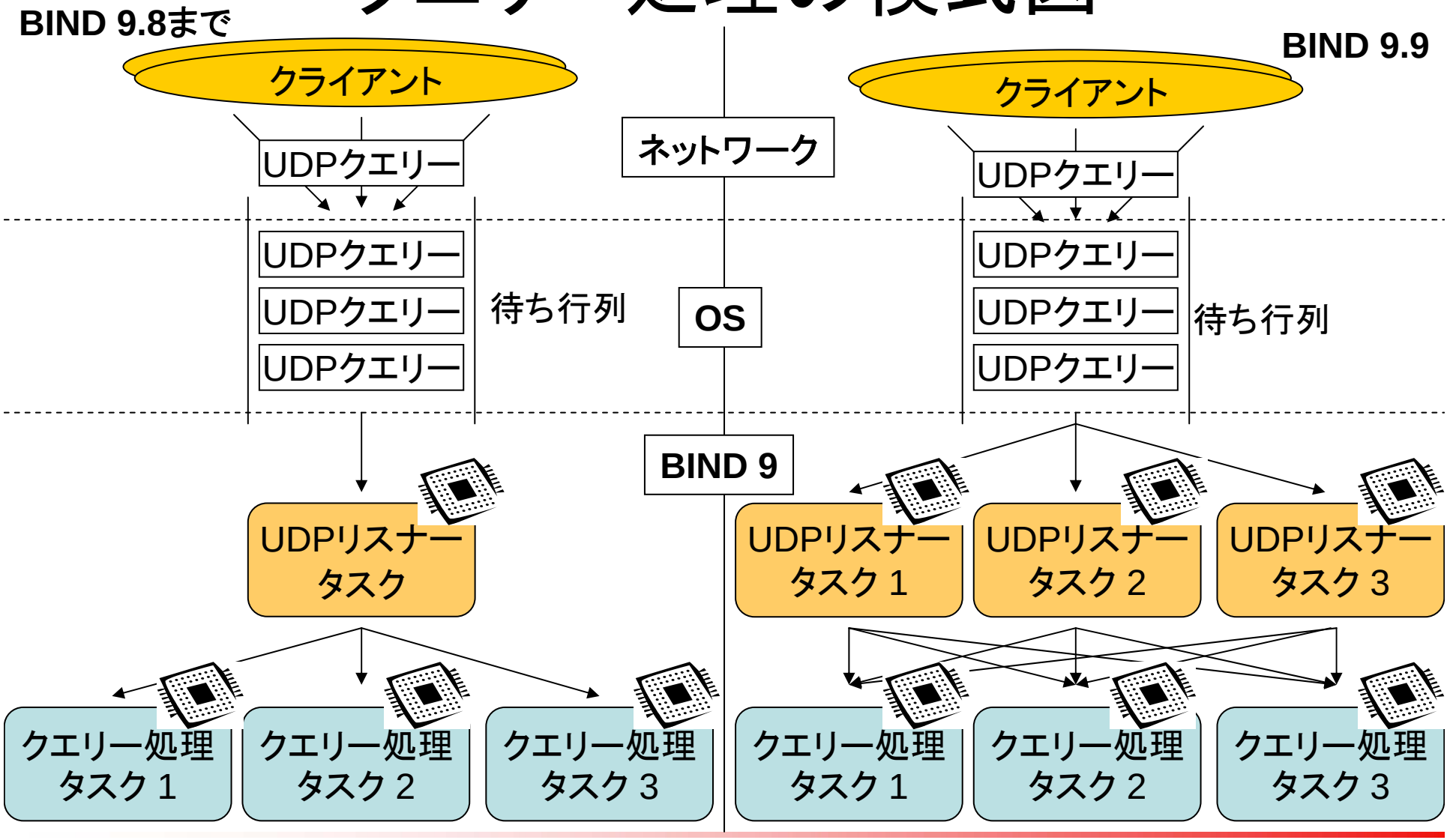
- ✓マルチスレッドI/O
- ✓rndcコマンドの機能追加
- ✓digの仕様変更
- ✓レコード順序のデフォルト値変更
- ✓クエリログのフォーマット変更

マルチスレッドI/O（1）
概要

- UDPソケット（listen-onで指定）からのDNSクエリの読み取り方法が変更
  - BIND 9.8までは、1タスク1ソケットを担当
  - BIND 9.9では、1ソケットに対して**CPUコアの数だけタスクを生成**
- **複数コア**を搭載したサーバーで、**性能向上**が見込める
- ソケットに対するタスクの数は起動オプション(-U)で変更可能
  - 上限値はCPUコア数

- **Windowsは対象外**
- Linuxでは**lockless UDP transmit path**のサポートが必要（Linux 2.6.39以降）

マルチスレッドI/O（2）
クエリー処理の模式図



rndcコマンドの機能追加

- flushtree

```
$ rndc flushtree <名前>
```

  - <*名前*>以下のツリーをキャッシュから削除
  - 例えば、example.jpと指定した場合、example.jpだけでなくwww.example.jpのキャッシュも削除

- sync

```
$ rndc sync
```

  - Dynamic Updateされたゾーン内容をディスクへ書き出す
  - 今までrndc freezeとrndc thawを組み合わせて実行していたことが**1コマンドで可能**になった

digの仕様変更

- オプションのデフォルト値が変更された
  - デフォルトで**DNSSECの検証結果要求とEDNS0が有効**になった
    - +adflag（DNSSECの検証結果を要求する）
    - +edns=0（EDNS0を有効にする）
  - +traceを指定すると、+dnssecも自動的に有効になる

- 表示に関するオプションが追加された
  - +[no]rrcomments: DNSKEYのコメントを表示／非表示
  - +split=X: 16進形式／Base64エンコードされたレコードの表示幅を指定
  - +nosplit: 16進形式／Base64エンコードされたレコードを1行で表示

レコード順序のデフォルト値変更

- レコード順序（RRSet ordering）とは
  - 応答として複数のレコードが返された際（www.example.jpに複数のAレコードが登録されている時など）の順番を指定する
  - BIND 9.9.0以前のデフォルトは”cyclic”なので、レコードは**同じ順序で循環**される
- BIND 9.9.0で、デフォルトが”random”に変更された
  - レコードの順序は**ランダム**になる
  - 下記オプションで**以前の挙動に戻せる**

```
options { rrset-order { order cyclic; }; };
```

  - アプリケーションが受け取る応答は、スタブリゾルバーの実装にも依存する

クエリログのフォーマット変更

- カラム（qname）が追加された
  - BIND 9.8系まで

```
client␣127.0.0.1#62536:␣query:␣example.com␣IN␣SOA␣+SE
```

  - BIND 9.9系

```
client␣127.0.0.1#62536␣(example.com):␣query:␣example.com␣IN␣SOA␣+SE
```

- クエリログ以外（security.logなど）にも付加される
  - ある特定のクエリを他の種類のログでもトラッキングできるようになる
- 設定ファイルではフォーマットを元に戻せない
  - ハードコーディングされているため、ログフォーマットを変更するにはソースコードを書き換えるしかない

2. バージョンアップ時の応答内容の比較

方法と条件

- 方法
  - 評価対象のnamedに対してクエリを送出
  - 応答内容をRRset順序整列、大文字小文字を揃えた上で違いがあるかを比較

- 条件
  - BIND 9.7.3-P3 と BIND 9.9.1-P1 で比較
  - ゾーン: .jpゾーンと同様のレコード数
  - クエリ:
    - RD bitは常にオフ、DO bitはオン・オフ両方のパターンを試す
    - qtype: A・AAAA・NS・DS・MX・TXT・RRSIG等
    - qname: ゾーンに存在する名前（+www等）、存在しない名前

結果

- DNSSEC未署名ゾーンに存在する名前に対するRRSIGの応答で挙動の変更あり
  - ➔RRSIGを直接聞くケースは、通常のリゾルバではないため問題ないと判断
- 上記以外は変化なし

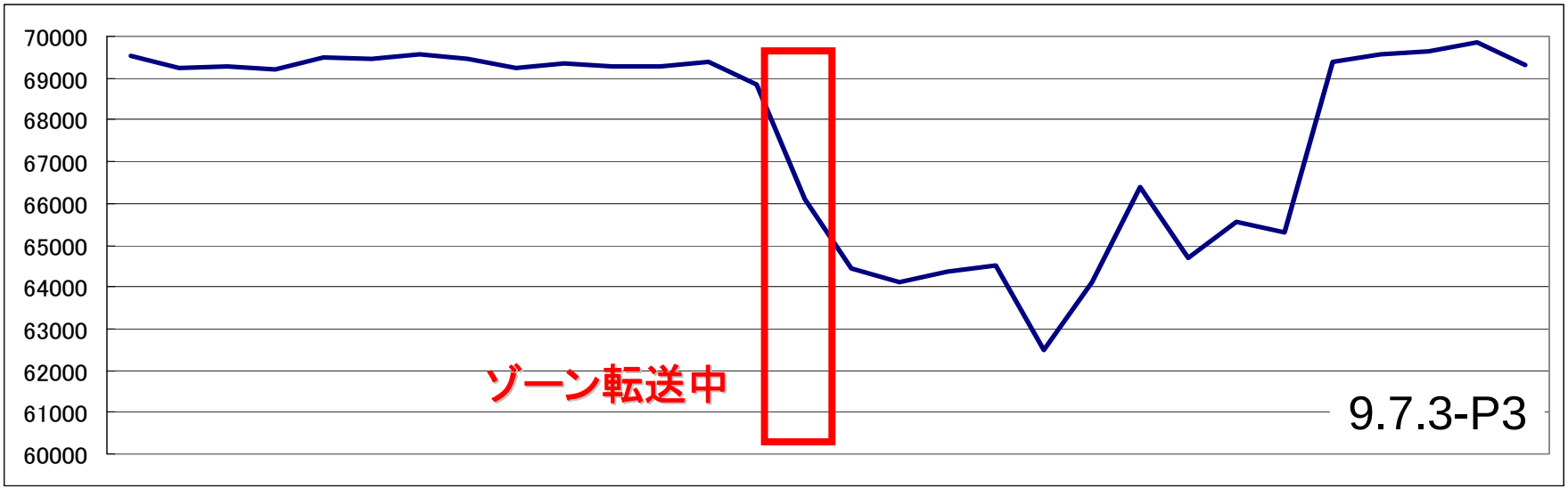
3. ゾーン転送中の
クエリ処理性能

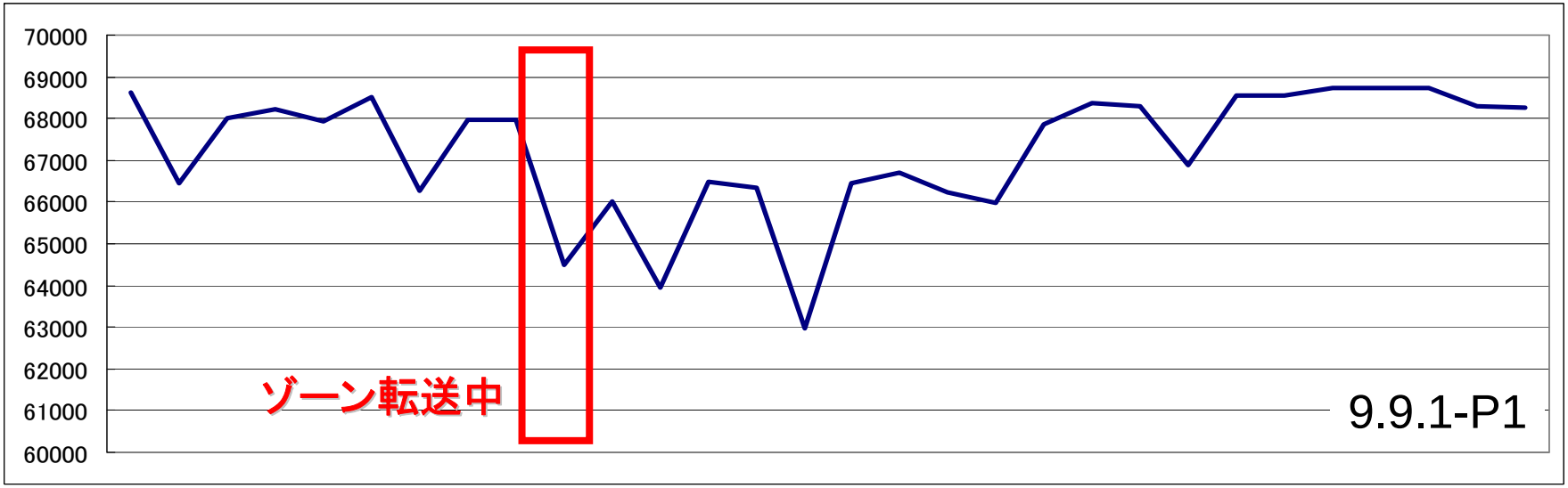
方法と条件

- 方法
  - 評価対象のnamedに対して、queryperfで送出
  - ゾーン転送中に実験を行い、転送による応答性能の低下があるかを確認

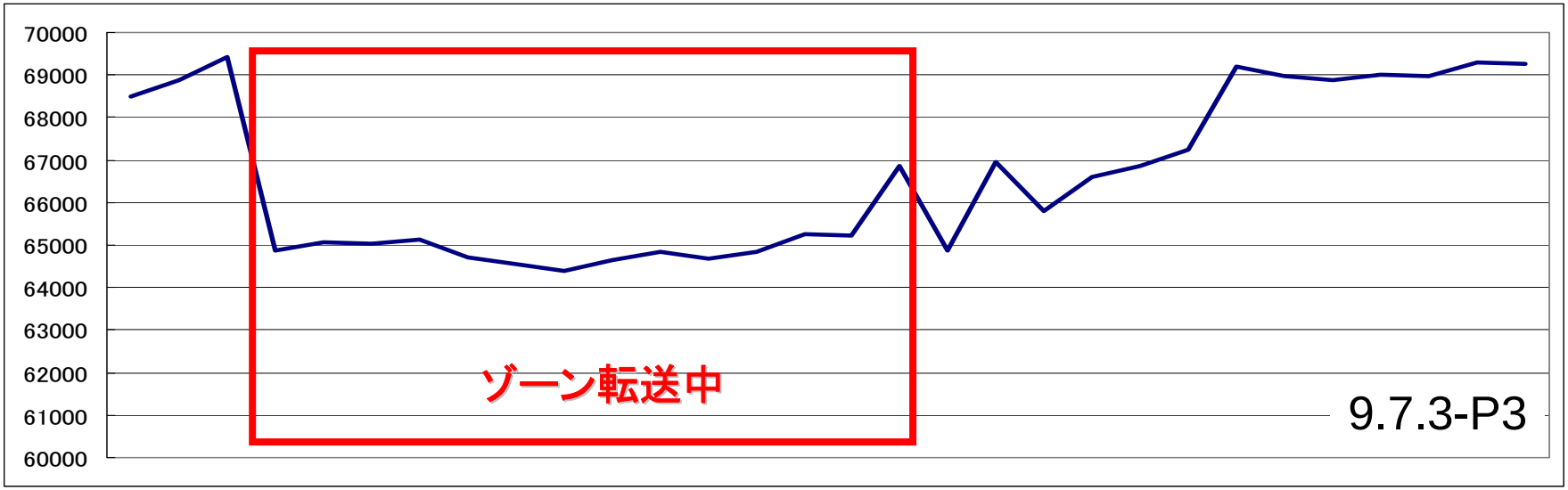
- 条件
  - BIND 9.7.3-P3 と BIND 9.9.1-P1 で比較
  - ゾーン: .jpゾーンと同様のレコード数
  - クエリ:
    - qtype: A・AAAA・NS・DS・MX・TXT・RRSIG等
    - qname: ゾーンに存在する名前（+www等）、存在しない名前
  - クエリログ: オフ

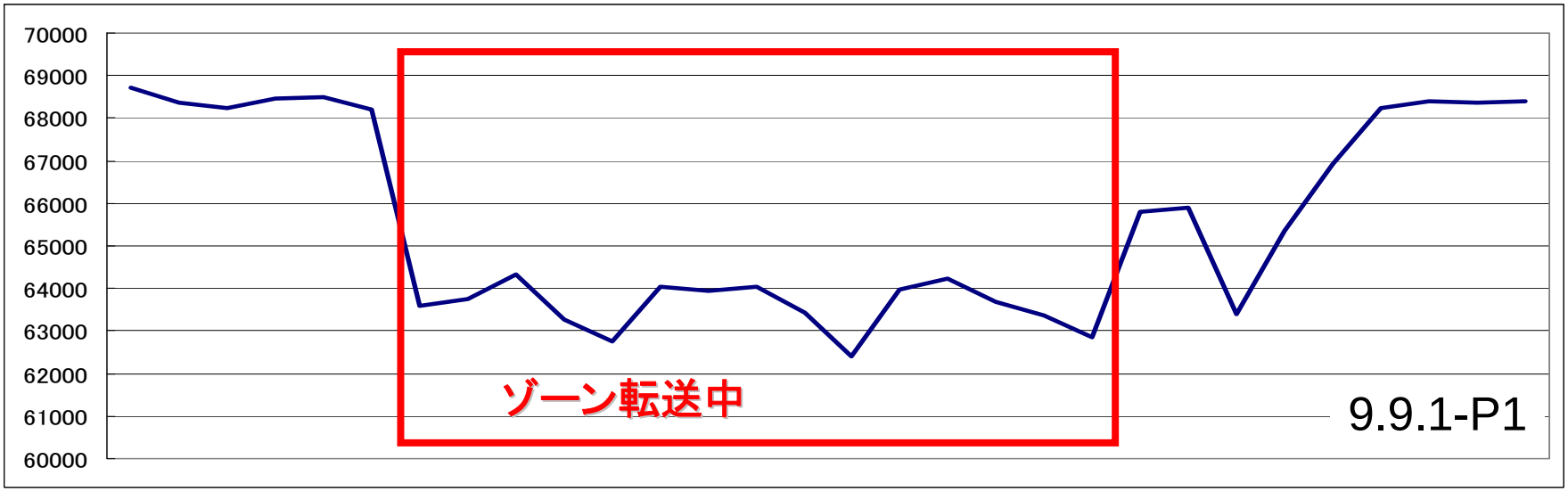
結果（1）差分転送（IXFR）





結果(2) 全量転送(AXFR)





結果(3) 考察

- ゾーン転送中の応答性能の低下については BIND 9.9.1-P1はBIND 9.7.3-P3に比べて若干の改善が見られる
- マスターからゾーンを受信した後も、しばらく応答性能が低下している状態が続いている
  - 内部データベースの更新のため？
- AXFRの実行中でも、応答が止まることはない

参考

- Internet Systems Consortium
  http://www.isc.org

- RFC 1918 (Address Allocation for Private Internets)
  http://www.ietf.org/rfc/rfc1918.txt

- RFC 6303 (Locally Served DNS Zones)
  http://www.ietf.org/rfc/rfc6303.txt