IPv６やセキュリティを考慮した高性能基盤アプリケーションの研究開発（041103003）

Research and Development of Key Internet Applications with IPv6 and Security Enhancement

神明　達哉　株式会社東芝　研究開発センター　通信プラットホームラボラトリー
Tatuya Jinmei　Corporate R&D Center, Toshiba Corporation

神田　充　江坂　直紀　小堺　康之
Mitsuru Kanda　Naoki Esaka　Yasuyuki Kozakai
株式会社東芝　研究開発センター　通信プラットホームラボラトリー
Corporate R&D Center, Toshiba Corporation

研究期間　平成 16～平成 17 年度

概要

本研究では、インターネットの基幹技術の一つであるドメイン名システム(Domain Name System, DNS)を主な対象として、次世代インターネットプロトコルやセキュリティ面への対応を考慮した高性能基盤アプリケーションを開発する。具体的には、DNS サーバの標準実装である BIND9 を用いて、IPv6 やセキュリティ拡張(DNSSEC)に対応できるだけの性能と機能を実現し、さらにその結果として、IPv6 対応の充実や DNSSEC 機能の普及を図る。サーバ性能のうち、応答性能については、複数プロセッサ環境での効果に注力し、1 プロセッサあたり 50%の向上を実現する。起動性能については従来実装の 2 倍に引き上げ、旧バージョンよりも高速化する。さらに、IPv6、DNSSEC といった応用技術を利用する高機能な DNS クライアントを新規に設計し、プロトタイプ実装を通じてその効果を検証する。また、以上の研究の成果はフリーソフトウェア形式で公開し、より広範囲の普及を目指す。

Abstract

We develop a high-performance Internet application targeting the Domain Name System (DNS) with consideration of supporting the next generation Internet, IPv6, and the security enhancement of DNS. Our engineering goal is to improve BIND9, the standard implementation of DNS, so that it can handle 50% of the single-processor query rate for every additional processor, it can load configurations twice as fast as before, and it can work as a base of DNS client applications for the richer functionality. We also publish the development result as free software for wider deployment of the new technologies.

１．まえがき

インターネットの発展とともに、その基幹機能である DNS への要求も高まっている。すなわち、ネット詐欺等の犯罪防止を実現するセキュリティ機能(DNSSEC)や、IPv6 等の新規技術への対応、またそれに耐えうる高性能なサーバが必要とされている。

しかし、DNS サーバの標準実装として広く使われている BIND9 では、サーバとしての十分な性能が実現できておらず、一方、クライアントにおいては、必要な機能を持つ実装が提供されてこなかった。本研究では、サーバの高性能化と高機能クライアントの実現によってこれらの課題を解決し、より高度な DNS 機能による次世代インターネット基盤の確立を目標とする。

具体的には以下を実現する。サーバの応答性能に関しては、マルチプロセッサ環境において、一プロセッサ時の応答性能に対し、プロセッサを一つ追加するごとに 50%ごとの向上を実現する。さらに、サーバの起動に要する時間を 2 倍以上に高速化する。一方、クライアントについては、一般アプリケーションから利用可能なライブラリの形で、IPv6,v4 が混在する環境における円滑な名前解決機能と、DNSSEC を用いたセキュリティ拡張を実現する。

さらに、これらの成果をフリーソフトウェアとして一般公開し、開発した応用機能の広汎な普及を目指す。

２．研究内容及び成果

2.1. サーバ応答性能の向上

本研究では、まず、スレッドを有効化した BIND9 サーバを複数プロセッササーバ上で動作させ、スレッド間の同期に要するオーバヘッドを測定した。その結果、応答メッセージを構成する際のメモリアクセスの競合、スレッド間で共有するデータオブジェクトへの参照カウンタおよび DNS のデータベースへのアクセスにおけるスレッド間のロック競合が支配的な要因であることを確認した。

そこで、これらのボトルネックを以下の方法によって除去した。

- メモリ管理用のデータ構造を実行スレッドごとに分離し、その間での競合を回避する。
- データ構造への参照カウンタをアーキテクチャ依存のアトミック操作で代替させ、カウンタにロックをかけることによるオーバヘッドを削除する。
- 同様に、読み書きロック（reader-writer lock）のバックエンドにアトミック操作を用いることで、書き込みのない（つまり典型的な）状況におけるロックのオーバヘッドを削除する。
- さらに、この機構をデータベースアクセス全般に利用することで、全般的な応答性能を向上させる。

次に、ルート DNS サーバとして動作させる設定において、実際のルートサーバへの問い合わせデータを用いて、スレッド数の増加が単位時間あたりに処理可能な問い合わせ数に与える影響を複数の実装間で比較した。この評価には AMD の Opteron プロセッサを 4 基搭載するサーバ機と 64 ビット対応の SuSE Linux 9.2 を用い、並列動作するスレッドを 1 から 4 まで変化させて性能を測定した。サーバ実装としては、従来および改良後の BIND9 に加え、BIND の旧バージョンである BIND8 を対象とした。

その測定結果を図 1 に示す。ここで、BIND9 の結果における”old, new”および”thread, nothread”は、それぞれ従来実装と改良実装、およびスレッド対応の有無を示す。

また、BIND8 および BIND9（no thread）においては、スレッド数の増加は結果に影響しないため、すべてのスレッド数において同じ性能が出ているものとしている。BIND9（new,thread,target）は、改良実装に対する本研究での目標値とした性能を記したものである。

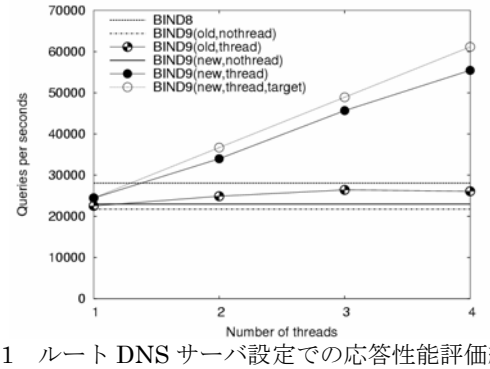

図 1　ルート DNS サーバ設定での応答性能評価結果

この結果によれば、本研究での改良実装は、目標としていた性能を概ね実現しており、旧バージョンの実装との比較においても複数プロセッサ利用時の優位性を示している。また、キャッシュサーバとしての動作時や、DNS の動的更新機能を利用する場合においても、同様の評価手法によりプロセッサ数に応じて目標値に近い、もしくはそれ以上の性能を示すことを確認した。

2.2. サーバ起動性能の向上

一方、サーバ起動性能の向上のために、本研究では、テキストベースのゾーンファイル(DNS サーバのデータ)をあらかじめ BIND9 の内部データ構造に近いバイナリ形式に変換しておき、起動時にバイナリファイルがあればそれを読み込むようにする手法を実装し、評価を行った。

本実装では、バイナリ形式において整数値をネットワークバイトオーダで保存するなどの工夫により高い移植性を確保した。さらにバイナリ形式ファイルを生成する方法として、サーバからダンプする方式に加え、テキストファイルを直接バイナリ形式に、あるいはその逆方向に変換できるようにする専用のツールも開発した。

本実装の性能評価として、2003 年 4 月時の.NET ゾーン（約 850 万レコード）を対象に、応答性能評価と同様のサーバ環境において、スレッドなし、スレッドありの両者についてゾーンファイルの読み込み時間を測定した(図 2)。この結果から、本研究によって改良した実装において目標通り従来比 2 倍以上の高速化が実現でき、また、旧バージョンに比べても優位であることが確認できた。

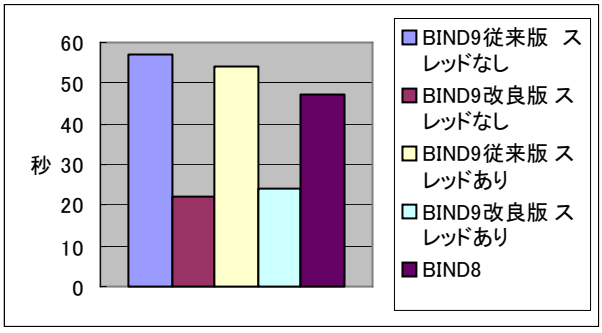

図 2　NET ゾーン読み込み時間の比較

本実装の成果は、前節で述べた応答性能に関する改良と合わせ、BIND9 の最新評価版であるバージョン 9.4.0a5 として 2006 年 5 月に一般に公開された。

2.3. 高機能クライアント開発

クライアント機能の基本設計として、本研究では、まず BIND9 サーバの内部で利用しているライブラリから DNS のプロトコル処理に関する部分を抜き出し、そのインタフェースを一般化するための中間層を提供してライブラリ化を実現するという方針のもとに検討、プロトタイプ実装を完成させた。

さらに、そのプロトタイプ実装のライブラリを SSH クライアントにリンクさせ、その動作を検証した。まず、IPv6 と IPv4 が混在する環境において、非同期な名前解決機能を利用して、IPv6 および IPv4 のアドレスを並行して求められることを確認した。IPv6 への移行途上においては、IPv6 アドレスに対する DNS の問い合わせを無視したり、そうした問い合わせに不正な応答を返したりするサーバの存在が知られている。こうしたサーバを利用している場合でも、名前解決を並行して行うことで、クライアント側での不要な待ち時間が削減できる。

一方、DNSSEC 機能を利用した名前解決においては、IP アドレスを求めるための DNS の問い合わせに不正な応答が得られた場合、これをライブラリ内で検出してアプリケーションにエラーを返すことで、アプリケーション側では不正なアドレスに対するコネクション接続が発生しないことを確認した。

本研究成果は BIND9 の開発元である ISC にフィードバック済みであり、将来の BIND9 の公開版に取り込まれる見込みである。

3．むすび

本研究で達成した成果により、DNS サーバにおいては IPv6 やセキュリティ拡張のような応用技術を DNS 上で展開するにあたって十分な性能が得られる。 また、クライアントにおいてはこうした応用機能を一般のインターネットアプリケーション向けにも適用できる基盤が実現された。その直接的な成果として、今後の DNS の運用がより高度化かつ安定すると考えられる。一方、DNS は、インターネットの根幹をなす機能の 1 つであり、メールや WWW をはじめ、インターネット上のほとんどすべてのアプリケーションが何らかの形で依存している要素技術である。本研究の成果がもたらす副次的な効果として、こうしたアプリケーションが DNS の拡張機能を自在に利用できるようになり、また DNS のセキュリティを利用した安全なアプリケーションの新規開発が促進されると期待できる。

【誌上発表リスト】

[1] Tatuya Jinmei, Paul Vixie, “Practical Approaches for High Performance DNS Server Implementation with Multiple Threads,” WIT 2005 (小倉)(2005 年 11 月 25 日)

[2] Shigeya Suzuki, Tatuya Jinmei, Sohgo Takeuchi, “Fixing DNS Misbehavior Hindering IPv6 Deployment,” SAINT 2006 IPv6 Workshop (Phoenix, USA) (2006 年 1 月 27 日)

[3] Tatuya Jinmei, Paul Vixie, “Implementation and Evaluation of Moderate Parallelism in the BIND9 DNS Server”, 2006 USENIX Annual Technical Conference (Boston, USA)(2006 年 6 月 1 日)

【申請特許リスト】

[1] 神明達哉、「通信装置、通信方法および通信プログラム、日本」、(2006 年 3 月 22 日)