論　文

10GbitEthernet 対応 URL フィルタリング装置の開発

坂巻　佳壽美*　　森　久直*　　乾　剛**　　高山　匡正***

Development of URL Filtering Device for 10Gbit Ethernet

Kazumi Sakamaki*,　Hisanao Mori*,　Takeshi Inui**,　Kunimasa Takayama***

The Network security systems have become is necessary for our society in recent years, and one of being URL Filtering devices. Now, the way of Filtering processing with software is currently the most popular. This method produces some results, but processing time is slow, so in the coming era of 10Gbps, it is impossible to handle, even using the fastest CPUs (microprocessors). Certainly, this method is useful and widely common. However it takes a lot of time if we used in this method, so it is not possible to correspond to CPU of the highest processing performance in the time of 10Gbps.

Thus in this paper research and development, we proposed investigated the method of the super high speed pattern match processing circuits, and made an experimental network URL filtering system for 10Gbps .As a result, this system's throughput was up to 1.6Gbps even if it have received in the worst case of receiving continuous minimum length packets that is worst case. In addition, it is achieved 6.0Gpbs when receiving throughput was up to 6.0Gbps when this system received continuous maximum length packets.

キーワード：URL フィルタリング，ネットワークセキュリティ，FPGA，ハードウェアフィルタリング，10Gbps，10GbitEther

Keywords: URL filtering, Network security, FPGA, Hardware filtering, 10Gbps, 10GbitEther

1.　はじめに

インターネットは身近で有効な情報収集手段として，すでに必要不可欠な存在になっている。たとえ，その利用に伴う危険性（ウィルス被害やＤｏＳ攻撃（Denial of Service attack）など）が予想されるとしても，もはやインターネットの利用を中止することは不可能と思われる。

この深刻な問題に対して，ネットワークを通過するパケットをある条件にしたがって遮断し，不正な情報の伝達を防ぐためのフィルタリング（トラブルの原因となる部分を取り除く処理）が有効であり，様々な研究･開発[(1)(2)]が行われているが，未だ完璧な対策は存在しない。

現在主流となっているのは，ソフトウェアによるフィルタリング処理である。しかし，この方法では，ある程度の成果を上げることができても，処理時間がかかるために，これからの 10Gbps 時代には，最速のＭＰＵ（マイクロプロセッサ）を用いたとしても対応しきれない状況にある。

さらに，今後も益々普及し発達し続けるインターネットインフラ[(3)]においては，10Gbps を超える通信速度への需要が高まっている。それに伴い，高速フィルタリング装置の市場要求も，ますます増えてくると考えられる。

そこで，本研究開発においてはフィルタリング処理の代表的な事例として，ホームページのアクセスなどの通信を対象としたURLフィルタリング処理について，10Gbps への対応を目標とした。そのために，全ての処理をハードウェア化して FPGA(Field Programmable Gate Array)上に実装した高速 URL フィルタリング装置の試作開発を行った。

2.　URL フィルタリング装置の試作

2．1　URL フィルタリング装置の構成　　今回開発した URL フィルタリング装置は，図１に示すように３枚のボードに分割して構成した。このうち両端の２枚の送受信ボードは同じボードであり，10GbpsEthernet の光信号を電気信号に変える O/E 変換およびその逆変換を行っている。中央のフィルタリングボードが，変換された電気信号を全二重シリアルトランシーバ（Rocket I/O）で受け取り，フィルタリング処理を実装するための大容量 FPGA を実装したボード

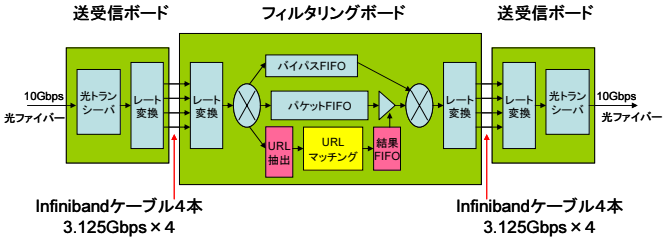

図１　フィルタリング装置の全体構成

＊　ＩＴグループ
＊＊　東京都水道局東村山上水管理事務所（前東京都立産業技術研究所）
＊＊＊　東京都交通局車両電気部（前東京都立産業技術研究所）

である。これらのボード間の接続には Infiniband ケーブルを４本用い，10Gbps のバンド幅を確保している。

2．2　フィルタリング処理　フィルタリング処理には，“IP アドレス”や“TCP ポート”といったイーサフレームの固定箇所だけチェックすれば良いものから，イーサフレームのデータ部（コンテンツ）までをチェックする必要のあるものまで様々である。そこで、今回の研究開発においては，代表的なフィルタリング処理である URL フィルタリングを対象とした。

URL フィルタリング処理とは，URL(Uniform Resource Locator,インターネット上のリソースを特定するための形式的な記号の並び，例えば http://www.yahoo.co.jp など)を元に，情報の通過の是非を判定する処理である。具体的な処理としては，HTTP プロトコルのリクエストパケットのヘッダ部分から，URL を抜き出し，URL のブラックリスト（有害な URL が収まっているデータベース）と比較し，一致した場合には，そのパケットを廃棄する処理である。

フィルタリング処理部のブロック図を図２に示す。

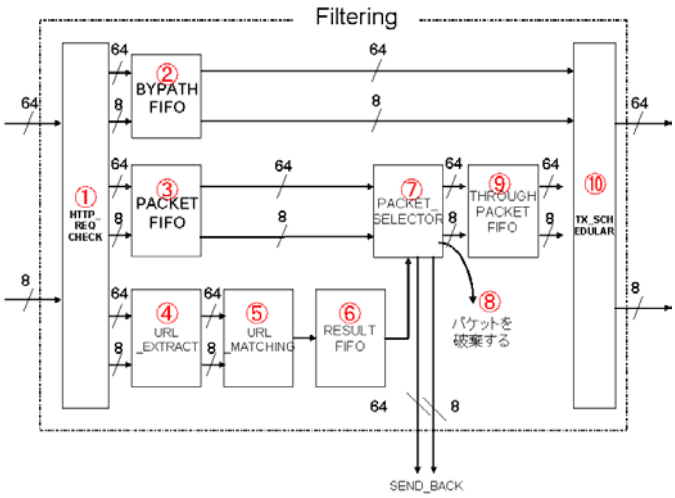

図２　フィルタリング処理部のブロック図

ここでのデータ処理の流れは以下の通りである。

①HTTP_REQ_CHECK で入力パケットが HTTP のリクエストパケットか判断する。

②リクエストパケットでなければ，BYPATH FIFO にデータを流す。

③リクエストパケットであれば，PACKET FIFO にデータを流すとともに，URL_EXTRACT にデータを流す。

④URL_EXTRACT では，パケットの中から URL を抜き出し，それを URL_MATCHING に流す。

⑤URL_MACTHING では，流れてきた URL を元にデータベースとのマッチング処理を行う（次章で詳述）。

⑥その結果（遮断対象か否か）を，RESULT_FIFO に流す。

⑦PACKET_SELECTOR では，RESULT_FIFO をみて，遮断対象であれば，PACKET_FIFO にある対象パケットのヘッダ部を，SEND_BACK に流したのち，

⑧そのパケットを廃棄する。(SEND_BACK では，通信を打ち切る返送パケットを生成する。)

⑨遮断対象でなければ，THROUGH_PACKET_FIFO にデータを流す。

⑩TX_SCHEDULAR では，BYPATH_FIFO と THROUGH_PACKET_FIFO をみて，データがあれば，通過パケットとして出力する。両方にデータがあった場合はラウンドロビン方式で出力する。

3.　マッチング処理の高速化

3．1　データ探索アルゴリズムの検討　フィルタリング処理の高速化で最も大きな問題は，URL ブラックリストの探索処理である。今日，URL ブラックリストは専門の会社から入手可能であり，内容は常時更新されている。その件数は，数十種類のカテゴリに分類されていて，数百万件～数千万件にも達している。

今回は URL フィルタリングにおける検索アルゴリズムとして，バイナリサーチを採用した。バイナリサーチ（２分木探索）は，ソート済みのサーチ空間の中央のエントリとキーを比較し，値が小さければ前半のデータを，大きければ後半のデータを採用し，キーがマッチするか比較要素が無なるまでこれを繰り返すという探索方式である（図３）。

バイナリサーチには，以下の特徴があり，本応用に適していると判断した。

①各次数における比較要素が固定している

②比較回数の上限が決まっている。

③そのため最悪ケースでのサーチ時間が予測できる。

④サーチ対象 N に対しての最大比較回数が $\log_2 N+1$ と少ない。

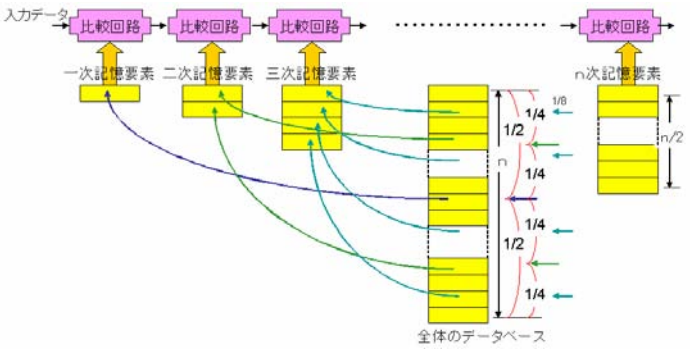

図３　バイナリサーチの動作

3.2　バイナリサーチの高速化　URL ブラックリストの件数が増大すると，それらの格納場所として SRAM や DRAM といった外部メモリを割り当てるが，その場合のアクセスタイムは FPGA 内部のレジスタや RAM（Distributed RAM，Block RAM など）に比べて多大な時間を要し，探索処理時間も増大することになる。

本試作開発では，遅延時間は問題とならないが，スルー

プットは最悪ケースに対応している必要がある。バイナリサーチは，初回の比較は必ず同一のエントリと比較され，以降は比較される可能性のエントリ数が２のべき乗で増えていくが，エントリ当たりの参照頻度は下がってくる。そのため，初期段階で比較されるエントリほど高速小容量のメモリに格納しておき，以降の比較候補のエントリにおいては、順次より低速大容量のメモリに格納することにする。このような考え方を“メモリ階層を考慮したバイナリサーチ”（特許出願中）と呼ぶことにする。FPGA の内部および外部にある各種メモリデバイスを階層化して利用した場合の、この考え方を図４に模式的に示す。

比較器は，最大比較回数分を用意しておき，入ってきた入力文字列を一定クロック数毎に次の比較回路へ移すというパイプライン化した構造（図５）にすることにより，高いスループットを実現することができた。この場合には，メモリ階層でのスループットを均一化する必要があり，かつメモリ階層間の比較回数を，メモリ容量とバンド幅を勘案し，データが同じペースで処理されるように工夫しなければならない。

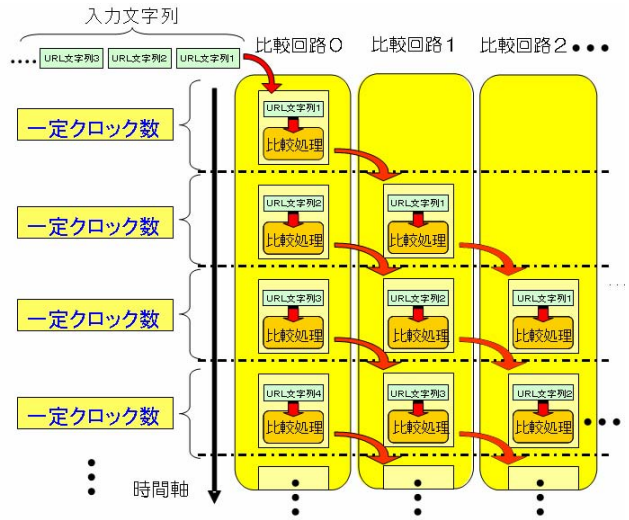

図４　メモリ階層を考慮したバイナリサーチの考え方

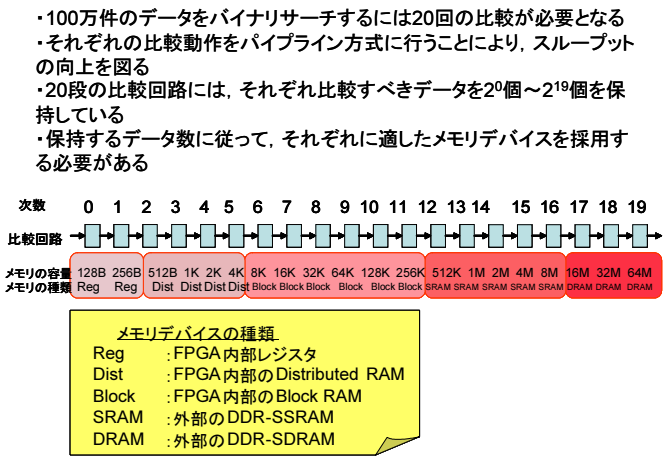

図５　比較回路のパイプライン化

3.3　メモリ階層を考慮した実装

これまでの検討をふまえ、以下のような要件で，URL フィルタリング装置を大容量 FPGA ボードへ実装するためのメモリ階層化への対応を行った。

- サーチリストサイズ：1600 万件（ブラックリスト相当）
- サーチキー長：128B（1 つの URL の長さ）
- データサイズ：2GB（128B×1600 万件）
- BRAM（FPGA 内臓メモリ）：1MB（dual port）
- SRAM（外付けメモリ）：36MB（22.5Gbps，4ch）
- DRAM（外付けメモリ）：2GB（20.0Gbps，2ch）

まず，1600 万件＝2^{24} であることから，最大比較回数は 25 回となる。ここで，SRAM には，36MB／128B＝280k＝2^{18} 件の URL が記憶できることから，19 回の比較処理を受け持たせることができる。したがって，DRAM に受け持たせる比較処理の回数としては，25 回－19 回＝6 回　でよいことになる。その結果，DRAM のバンド幅としては，20Gbps×2ch／6 回≒6.7Gbps となる。

一方，BRAM には，1MB／128B＝8k 件の URL が記憶できることになるが，FPGA の本来機能である回路構成用にも使用するため，4k 件の URL を記憶させることにする。4k＝2^{12} であるから，始めの 13 回の比較を BRAM に受け持たせることにする。よって，SRAM の受け持ち回数の内，最初の 13 回がなくなることから，SRAM での比較回数は 19 回－13 回＝6 回に減る。その結果，SRAM のバンド幅は，22.5Gbps×4ch／6 回＝15Gbps となる。

ちなみに BRAM のバンド幅は，FPGA での 1 比較 100MHz と遅めに見積もったとしても，100MHz×128B×8bit×2（dual port）＝200Gbps　となり，BRAM のバンド幅は，200Gbps／13 回＝15.4Gbps となる。

以上から，DRAM でのバンド幅が比較処理のボトルネックとなり，システム全体の性能としては 6.7Gbps となることが分かる。しかし，インターネット上を流れるパケットには URL 以外の情報が多数あることから，実際には 10Gbps の通信速度を本装置でフィルタリング処理したとしても，スループットを低下させることはないと思われる。

4.　試作機の性能

試作したフィルタリング装置（図６）について，評価試験機[4]（本研究にて，（独）産業技術総合研究所が担当し，試作した。）を用いて性能測定を行った（図７）。この場合の最大のスループットは、パケット長の最小から最大までの範囲について、それぞれのパケット長における最小ギャップ長を求めることにより決定した。結果を表１に示す。パケット長が長くなるほど，スループットが向上していることが分かる。また，DRAM がボトルネックとなって生じる本システムの理論値である 6.7Gbps に近い結果が得られている。

今回のテストパケットは，全てをフィルタリング対象（HTTP_REQUEST パケット）で構成しているが，実際の

ネットワーク上の通信においては，フィルタリング対象外（ICMP，ARP，POP プロトコルなど）のパケットも含まれているため，更に高いスループットが見込まれる。

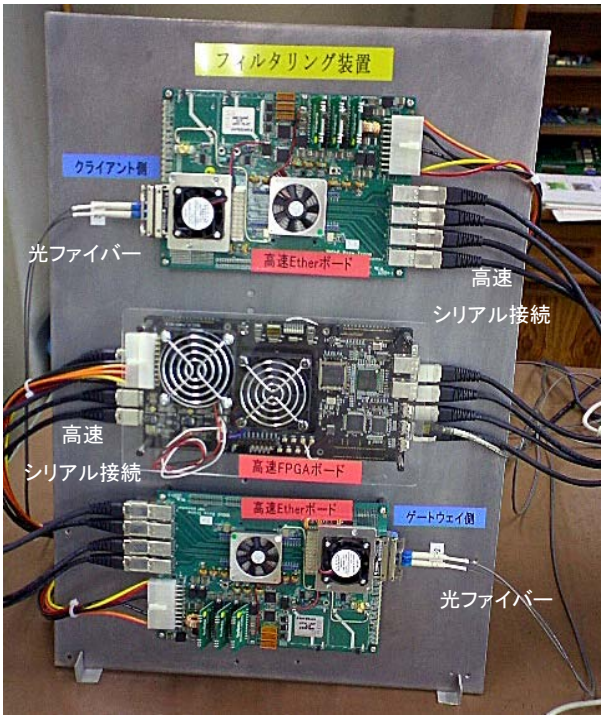

図６　試作したフィルタリング装置の外観
上から，送受信ボード，フィルタリングボード，送受信ボード．
ボード間は，4 本の Infiniband ケーブルで接続されている

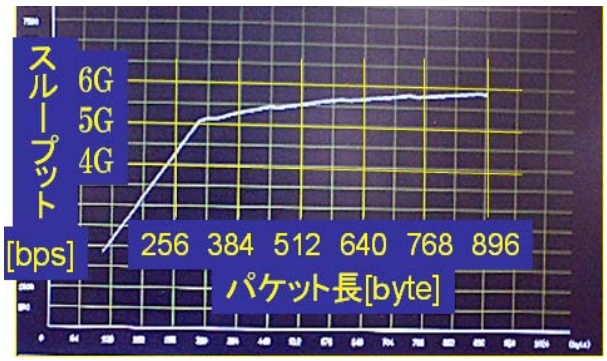

図７　評価試験実施中の表示画面

表１　試作したフィルタリング装置の性能

	平均パケット長 (byte)	限界パケット間隔 (byte)	スループット (Mbps)
①テストパケット1（最小）	99.39	288	1642.0
②テストパケット2	272.39	112	4535.2
③テストパケット3	998.39	96	5838.6
④テストパケット4（最大）	1505.39	96	6016.3

使用したテストパケットの構成は、
　ヘッダ＋"GET / HTTP1.1" + "Host: " + URL 名のみ
テストパケットの長さは、
　テストパケット１：平均 100byte
　テストパケット２：平均 270byte
　テストパケット３：平均 1kbyte
　テストパケット４：平均 1.5kbyte

5.　まとめ

本研究では，10GbitEthernet 対応の URL フィルタリング装置を試作開発した。10GbitEthernet の高速通信に対応するに当たり，フィルタリング処理におけるバイナリサーチをパイプラインで処理するために，「メモリ階層構造を生かしたバイナリサーチ」を考案し，FPGA への実装を行った。

その結果，ワーストケースである最小パケットの連続送信でも 1.6Gbps，最大パケット連続送信で 6.0Gbps のスループットを達成できた。

なお，本研究は平成 16～17 年度経済産業省地域新生コンソーシアム研究開発事業「パターンマッチング回路の超高速化とフィルタリング装置への応用」[5] の一環として実施したものである。コンソーシアムのメンバーである（独）産業総合技術研究所，デュアキシズ（株），（株）ビッツの関係者の皆様に深く感謝する。

（平成 18 年 10 月 25 日受付，平成 18 年 11 月 28 日再受付）

文　　献

(1) Kartik Gopalan, Tzi-cker Chiueh, “SBFilter: A Fast URL Filter Engine for Internet Access Management”, ESCL Technical Report TR-57, Computer Science Dept, Stony Brook University, Stony Brook, 1999.

(2) John W. Lockwood, Christopher Neely, Christopher Zuver, James Moscola, Sarang Dharmapurikar, David Lim, “An Extensible, System-On-Programmable-Chip, Content-Aware Internet Firewall”, FPL 2003, Lisbon, Portugal, Paper 14B, Sep 1-3, 2003.

(3) 高度情報通信ネットワーク社会形成基本法（「ＩＴ基本法」）（平成 12 年 11 月 29 日成立）

(4) 片下敏宏，坂巻佳壽美，　乾剛，名古屋貢，戸田賢二，“ネットワークフィルタリング試験装置の試作”，信学技報 CPSY2004-98，pp. 49-53，2004.

(5) 平成１７年度地域新生コンソーシアム研究開発事業「パターンマッチング回路の超高速化とフィルタリング装置への応用」成果報告書，平成 18 年３月