情報処理学会論文誌 Vol. 49 No. 6 2118–2128 (June 2008)

10 Gigabit Ethernetに対応したネットワークフィルタリング試験装置

片下敏宏[†1] 坂根広史[†1]
堀 洋平[†1] 戸田賢二[†1]

近年のネットワーク社会においてはセキュリティシステムが必須となっているが，その１つとして特定のフレームを遮断することにより安全性を高めるネットワークフィルタリングシステムがあげられる．ネットワークフィルタリングシステムはその用途に応じて様々な装置が研究開発されているが，それらの研究開発において機能試験や性能測定などの評価が欠かせない．特に高い負荷による評価はシステムの脆弱性の検証に重要であるが，現状ではバックボーンネットワークなどで利用される 10 Gigabit Ethernet のワイヤスピードで機能検証を行うことが困難となっている．そこで本論文ではフィルタリング装置の機能試験を高速に実施する試験手法を提案する．提案手法はハッシュテーブルを用いた送受信フレーム検査による高速な試験をハードウェアにより実現可能とし，さらに，小規模なハードウェア資源で実装が可能であるという特長を持つ．本論文では提案手法を用いて 10 Gigabit Ethernet に対応する試験装置の実装を行った．そして，URL フィルタリング装置や IPS（Intrusion Protection System）の開発において本試験装置を用いて機能試験や性能測定の評価を行い，提案手法による試験の有効性を示した．

A Novel Test System for Network Filtering Systems on 10 Gigabit Ethernet

Toshihiro Katashita,[†1] Hirofumi Sakane,[†1]
Yohei Hori[†1] and Kenji Toda[†1]

In this paper, we present a novel network test system that runs a verification of network filtering systems with evaluating their performance on 10 Gigabit Ethernet. The network filtering system is one of the network security systems and has been studied such as a firewall, a spam-mail filter, a contents filter, an URL filter, and an intrusion protection. In order to research and develop such systems, it is essential to evaluate their performance and capability. Particularly, measurement of the filtering performance is significant to examine their architecture. However, it was difficult to execute the evaluation appropriately because the performance and accuracy could not be evaluated at 10 Gbps wire speed by prior test environments. We propose a novel test method that verifies the filtering capacity and evaluates the performance of network filtering systems all at once by means of a hardware-based hash table. We implemented our method on an FPGA board equipped with a 10 Gigabit Ethernet interface. We also conducted the performance evaluation and the verification of the filtering capability for a URL filtering system and an intrusion protection system.

1. はじめに

コンピュータネットワークによるサービスは我々の社会に欠かせないものとなっているが，一方，利用者の増加などによりサービスに対する攻撃や侵入，不正な情報の流出などの問題が顕在するようになった．このため近年ではネットワークにおけるセキュリティが重要となっているが，そのネットワークセキュリティの１つの方策として，ネットワークトラフィック中のフレームを特定の条件に従って遮断することにより不正な情報の伝達などを防ぐフィルタリングがあげられる．ネットワークフィルタリングシステムはその用途に応じてファイアウォールや迷惑メールフィルタ，URL フィルタリング，IPS（Intrusion Protection System）など様々な装置が研究開発されている．

このようなフィルタリング装置の研究開発において，機能試験や性能測定の評価を通じたシステムの検証が欠かせない．特に，新しいアルゴリズムやシステム構成の脆弱性・有効性の検証においては，高い負荷による機能試験が重要である．しかし，従来は 10 Gigabit Ethernet のワイヤスピードで様々なトラフィックを用いたフィルタリング装置の機能試験を行うことが困難であった．これは，フィルタリングの機能試験が汎用コンピュータ上で tcpdump や tcpreplay プログラムを用いて実施されており，低速な試験しか行えなかったからである．汎用コンピュータによる機能試験が低速である理由の１つに，転送される莫大なフレームを単純に記録して検証を行っていたことがあげられる．この検証手法は巨大な記憶領域が必要であり，長時間にわたる試験も実施できないという問題もある．性能測定はトラフィックジェネレータなどを用いて実施されており，フィルタリングの削除対象ではない

†1 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology

© 2008 Information Processing Society of Japan

トラフィックによる測定がなされていた[1]．この性能測定はフィルタリング装置の厳密な性能を示すには妥当な方式であるが，システムの脆弱性の評価では削除対象のフレームが含まれた高負荷時の挙動など様々な条件の下で性能を検証することが求められる．

そこで本論文では，ハッシュテーブルを用いてトラフィック中のフレームを判別する方法をハードウェアで実装することにより，フィルタリング装置の機能試験を 10 Gigabit Ethernet のワイヤスピードで実現する手法を提案する．本手法は試験中に転送されるフレームそのものを記録するのではなく，フレームからハッシュ値を算出し，その値が指すテーブルの値を加算することによりフレームが転送された個数のみを種類別に記録する．そして，フィルタリング装置の入出力フレームそれぞれの個数を記録したハッシュテーブルを比較し，フレームが正しく遮断もしくは転送されているか評価する．試験時には転送するフレームの種類をあらかじめ定めておき，そのフレームを無作為に転送してトラフィックを生成することでハッシュテーブルを固定長かつ小規模な大きさに抑えている．すなわち，長時間にわたるトラフィックを用いてもテーブルの比較時間を固定かつ短く抑えることが可能であり，これにより長時間にわたる高速な機能試験を実現している．なお，ハッシュテーブルの衝突はあらかじめ試験に使用するフレームを調整することにより回避しており，フレームの転送個数が誤って記録されることはない．

本論文では提案手法を用いて 10 Gigabit Ethernet 用の試験装置を実装し，URL フィルタリング装置や IPS 装置の開発における評価試験に利用した．その結果，URL フィルタリング装置ではプロトタイプ装置のボトルネックとなっている原因を発見できたほか，様々な不具合を迅速に修正することが可能となった．また，IPS 装置では機能や性能を検証できたほか，長時間にわたる負荷試験によりプロトタイプ装置の信頼性を示すことができた．

2. フィルタリング装置の試験手法

フィルタリングのアルゴリズムやシステム構成の研究開発において，特定のフレームのみが遮断されて他のフレームは通過するかどうかを確かめる機能試験や，スループット計測による性能試験は，バグの抽出やフィルタリング装置の有効性を示すうえで欠かせない．

本研究ではネットワーク向けのフィルタリング装置を対象としているが，ネットワークの試験におけるフレームの測定方式には，試験用のフレームを生成してネットワークへ注入するアクティブ測定とネットワーク上で実際に通信されているフレームを観測するパッシブ測定があげられる．装置の研究開発の段階における試験においては，実際のネットワークに接続せずに実施できるアクティブ測定方式が適切であることから，本研究ではアクティブ測定を用いることとした．

本論文における機能試験では，フィルタリングの機能とネットワーク装置としての機能を評価することを対象としている．機能試験では様々なパターンのトラフィックを試験対象へ入力し，出力トラフィックを検証することで決められたフレームのみが遮断されフィルタリングが正しく機能しているか評価を行う．また，破損したフレームなどが入力された場合にフレームを破棄しつつ動作を継続することが可能であるかといった評価を行う．また性能試験は，フィルタリング装置がフレームを欠落させず処理できる入力トラフィックのスループットを測定することを対象としている．性能試験では試験対象のバッファなどによりトラフィックが蓄積されると本来の性能以上のスループットを計測してしまう可能性があるため，適度な長さのトラフィックを用いて実施する．

このような機能試験や性能試験を実施する従来の試験手法として，汎用コンピュータや専用試験装置を用いる方法があげられる．汎用コンピュータを用いた試験では，tcpreplay コマンドによりトラフィック生成を行い，試験対象からの出力を別のコンピュータで tcpdump コマンドにより記録した後に検証を行っていた[1),2)]．しかし，汎用コンピュータによるネットワークインタフェースの通信速度は特に短い長さのフレームで 10 Gbps を大きく下回り[3)]，この速度に制限された試験しか実施できなかった．つまり，広く普及しているコマンドにより容易に試験を実施できる方法であるが，10 Gbps といった高速なトラフィックによる試験を行うには不適であった．

専用装置による試験では，フィルタリング装置で遮断対象ではないフレームのみで構成されたトラフィックによってスループットの計測がなされていた[1]．つまり，計測時にフレームが欠落しないようなトラフィックによる計測であり，フィルタリング処理によりフレームが遮断される際の性能は計測することができなかった．一般的にフィルタリング対象ではないフレームはすべての対象ルールに照らし合わせられることから，フィルタリング装置のフレーム検査速度の評価として従来の方法は妥当である．しかし，システムの脆弱性やバグを検出するにはフレームがルールと一致する場合の装置の挙動を検証することも重要となるが[⋆1]，従来の方法ではフレームがフィルタリング対象であった際の通知や遮断する機構が働くと性能にどのような影響があるか検証することができなかった．

以上で述べたネットワーク装置の試験方法のほか，研究開発における装置の試験方法としてコンピュータ上での回路シミュレーションがあげられる．回路シミュレータ上であれば

⋆1 フレームがルールと一致すると，結果を通知する処理のために処理が低速となってしまう場合もある[4)]．

© 2008 Information Processing Society of Japan

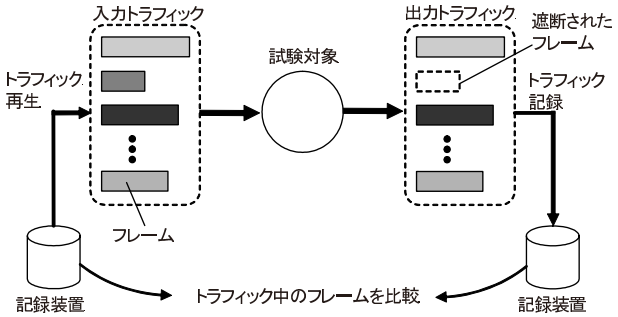

図 1　従来の試験手法
Fig. 1　Previous test method.

様々な形式・速度のトラフィックを仮想的に生成でき，装置の詳細な動作を検証することが可能である．しかしシミュレーション処理は低速であり，実時間で数秒のシミュレーションに数時間要するために，多様な条件をもとにバグや速度低下の問題点を抽出するには非常に長い時間を費やしてしまう．

そこで，ハードウェアによりトラフィックの生成とフレームの判別を高速に処理することで多様なトラフィックにより試験を実施してバグや速度低下の問題点などを絞り込み，その後に回路シミュレーションにより原因を特定するという方法が考えられる．

本論文で対象とする機能試験や性能試験は，試験対象の入力トラフィックと出力トラフィックを比較することにより実施することができる．しかし，**図 1** に示すような入出力トラフィックをそのまま記録して比較する手法は莫大な記憶領域と処理時間が必要であり，従来の tcpreplay や tcpdump コマンドに相当する機能をハードウェア化しても高速に試験を実施できない．このほか，数分程度の試験には 10 Gbps のワイヤスピードを考えると数百 GB の記憶領域が必要であるが，低速なハードディスクは数十台を並列化する必要があり[⋆1]，また，DRAM のようなメモリでも容量確保のため数十個のモジュールが必要となるが，いずれもハードウェアの IO パッド個数の制限により実現が困難である．

したがって，フレームの一部の情報をもとにトラフィックを比較することにより記憶容量を低減する対策が考えられる．その 1 つの手法としてフレーム中のあるデータを ID とし

⋆1 ハイエンドの製品でも連続アクセス速度がおよそ 580 Mbps である[5]ので 18 台以上を完全に並列化する必要がある．

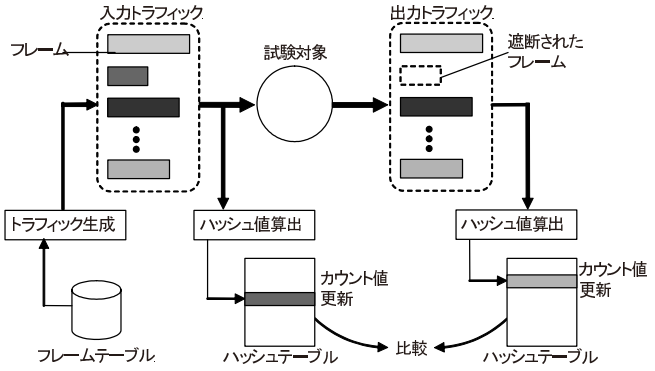

図 2　提案する試験手法
Fig. 2　Proposed test method.

て利用することでフレームを判別する方法が考えられるが，MAC 層を搭載した IDS を検査するような場合に用いることができない．IDS では IP パケットから ARP フレームまで様々なフレームを扱うため，ID に利用できるデータが MAC アドレスか CRC だけとなるが，MAC 層を搭載した装置では MAC アドレスや CRC が試験結果に影響するために使用できないわけである．

そこで本論文では，ハッシュテーブルを用いたフレームの判別機構を利用し，これをハードウェアで実装することにより高速かつ柔軟な試験を小規模なハードウェアで実現可能とする手法を提案する．

図 2 に提案手法による試験の手順を示す．提案手法では，まず，あらかじめ定めた種類のフレームをフレームテーブルに格納し，フレームテーブルから無作為に取り出したフレームの組合せにより入力トラフィックを生成する．そして入力トラフィック中のフレームから順次ハッシュ値を算出し，その値の指すハッシュテーブルのエントリを加算して更新することにより，フレームの転送された個数のみを記録する．試験対象から出力されたトラフィックからも入力トラフィックと同様にハッシュ値をフレームから順次算出し，トラフィック自体は破棄する．最後に，入出力ハッシュテーブルを比較することで，フレームが正しく遮断もしくは転送されているかを検証する．入出力トラフィック自体ではなくトラフィック中のフレームの転送数を比較するため，長時間にわたる試験においても記憶領域や処理時間を固定かつ小さく抑えることが可能となる．

ハッシュを用いたパケットの判別を用いて実ネットワークの遅延を測定する研究がなされ

© 2008 Information Processing Society of Japan

ている[6] が，これは実ネットワークを対象としたパッシブ測定であり，本研究の対象とするネットワークフィルタリング装置の試験に用いることができない点において異なる．

本手法ではハッシュテーブルの衝突によりフレームの転送数が誤って記録されることを避けるため，試験に用いるフレームを生成する際にあらかじめハッシュ値を算出しておき，これが各フレーム間で衝突しないようにフレームのデータを調整して回避する．データの調整にはペイロードに設けた専用の領域や試験に影響しないフィールドを用いる．試験で使用するフレーム間で衝突があり，かつ，データの調整が試験に影響するような場合には，該当フレームを削除する必要がある．

ハッシュテーブルにはフレームの転送された個数のみが記録されるため，トラフィック転送中のどの時点で不具合が起きたという情報を得ることはできない．ただし，トラフィック中のフレームが原因となっているかは分かるため，トラフィックのサブセットを生成して原因の絞り込みが可能である．

3. 試験装置の実装

提案手法による試験回路を FPGA ボード上に実装し，10 Gigabit Ethernet 向けのネットワークフィルタリング試験装置を構成した．本実装は，フィルタリング装置のバグやボトルネックを抽出し，その原因を回路シミュレータで早期に特定できる環境を構築する目的で行った．本試験装置には主に以下の 5 つの特徴 (1) 10 Gigabit Ethernet のワイヤスピードで機能試験と性能試験を実施，(2) 様々な試験トラフィックを制御 PC から柔軟に設定することが可能，(3) 制御 PC と連携して長時間にわたる試験を自動的に実行，(4) 回路クロック単位の高精細な制御，(5) 試験トラフィックを回路シミュレータのフォーマットで出力可能，を持つ．

図 3 に実装環境の写真，**図 4** に構成図を示す．試験装置の回路を搭載する FPGA ボードには Xilinx 社 Virtex-II pro 100 スピードグレード 6[7] が搭載されており，2 基の DDR SDRAM の SO-DIMM スロットと 4 基の 38 Mbit の DDR SSRAM を備えている．ネットワークインタフェースとして 2 基の 10 Gigabit Ethernet インタフェースボードが接続されており，10 GBASE-SR 光モジュールの XAUI（10 gigabit Attachment Unit Interface）信号を 4 本の Infiniband ×1 ケーブルを通じて伝送している．Infiniband ×1 の規格ではスループットが 2.5 Gbps（データ 2.0 Gbps）であるが，FPGA の高速 IO のパラメータ調整により 3.125 Gbps（データ 2.5 Gbps）で伝送することが可能であり，4 本で 10 Gbps のスループットを達成している．

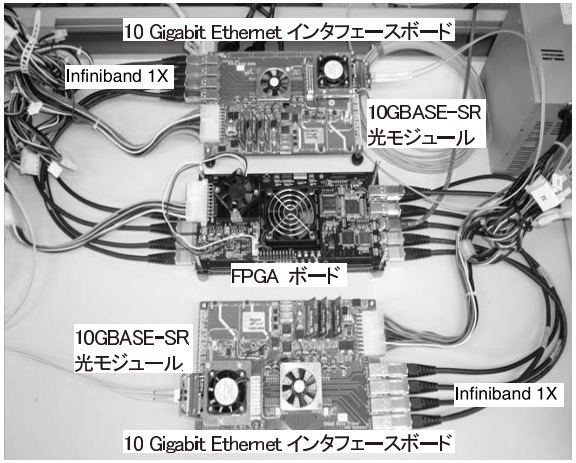

図 3　実装環境の写真
Fig. 3　Photograph of the evaluation system.

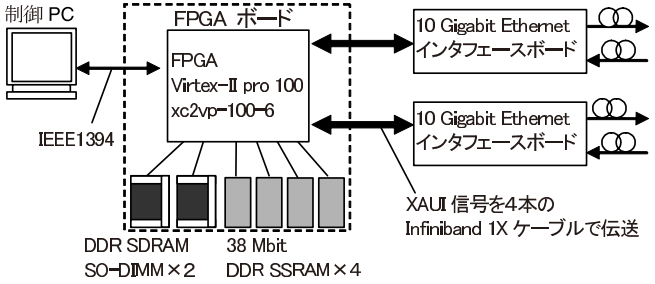

図 4　実装環境の構成図
Fig. 4　Structure of the evaluation system.

図 5 に実装した試験装置のブロック図を示す．本装置は主にトラフィック生成部と，トラフィック検査部から構成されている．

トラフィック生成部では，まず試験前に制御 PC 上でフレームを生成し，DDR SDRAM 上のフレームテーブルに登録する．そして試験時にテーブルからフレームを無作為に選択し，あらかじめ設定した長さのギャップ（Inter Frame Gap）を付加してトラフィックを生成し，試験対象へ送出する．フレームテーブルは分割して利用することが可能であり，複数

© 2008 Information Processing Society of Japan

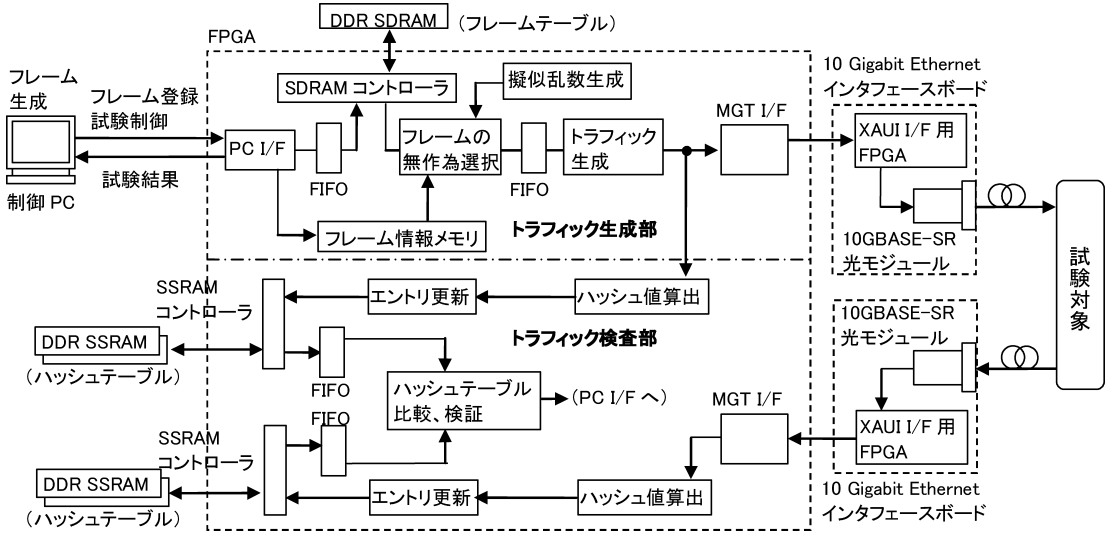

図 5　試験装置のブロック図
Fig. 5　Architecture of the evaluation system.

の性質のトラフィックを切り替えて試験を行うことが可能となっている．フレーム情報メモリには各フレームの長さのほか，フィルタリング装置で遮断されるかどうかを示すビットが記録されている．このビットは入力トラフィックとあわせてトラフィック検査部に転送し，ハッシュテーブルの検査時に各フレームがフィルタリング対象かどうかを判断するために用いられるもので，制御 PC 上でフレームを生成する際にフィルタリング装置の設計情報をもとに設定する．

トラフィック検査部では，入出力トラフィックからそれぞれハッシュ値を算出し，DDR SSRAM 上のハッシュテーブルのエントリを加算して順次更新する．入力トラフィックのテーブルにはフィルタリング対象かどうかを判断するためのビットが付加される．そして試験終了時に，遮断対象でないフレームのエントリは両テーブルが同じ値であり，遮断対象のフレームのエントリは出力トラフィックのフレームのエントリが 0 となっていることを検査し，結果を制御 PC へ出力する．このとき，遮断対象のフレーム，対象でないフレームの個数を入出力トラフィックそれぞれについて集計し，試験において転送されるべきフレーム数と一致するか検査を行う．このようにハッシュテーブルの検査はハードウェア上で自動的に行われるが，試験対象で不具合が起きた場合にどのフレームが原因となっているかを検証する際にハッシュテーブル全体を制御 PC へダンプすることも可能である．

長時間にわたる試験を実施可能とするためハッシュテーブルは 2 重化されており，一方のテーブルで試験を行っている間にもう一方のテーブルを比較・検証することが可能となっている．このテーブルを切り替えることで，同一のトラフィックを繰り返して負荷試験を連続的に実施できるが，切替え時にはガードタイムを設けてテーブルの更新の終了を待つ必要がある．ガードタイムはトラフィック生成部からフレームが送出されてから出力トラフィックのテーブルが更新されるまでの時間であり，主に試験対象のレイテンシの影響を受ける．ハッシュテーブルの比較時間より 1 回の試験時間の方が短い場合は，比較が終了するまで次の試験が待機するようになっている．

ハッシュ値の算出はフレームのチェックサムに使用されている CRC-32 を用いて，フレーム中の FCS（Frame Check Sequence）を除いたデータより算出している．可変長のフレームから CRC-32 を 10 Gbps の速度で算出するため，パイプラインによる高速化を施した論文 8) の手法による回路を用いている．

© 2008 Information Processing Society of Japan

表 1　試作した試験装置の主な性能
Table 1　Characteristic of the network tester.

フレームテーブル	65536 エントリ フレーム長 64 byte〜16 Kbyte （DDR SDRAM 1 Gbyte）
送出フレーム数	トラフィックあたり最大 2^{32} フレーム
繰返し試験回数	試験あたり最大 2^{32} 回
フレーム間ギャップ	12.8 ns〜約 107.4 ms 6.4 ns 間隔で調整
ガードタイム	12.8 ns〜約 6.7 ms 6.4 ns 間隔で調整
ハッシュテーブル	65536 エントリ エントリ長 32 bit （DDR SSRAM 256 Kbyte）

試験装置の回路は Xilinx ISE 8.2 sp2 で論理合成しており，回路規模は 6015 Slices，6937 LUTs，7718 FFs，107 BRAMs となり，最大動作周波数は 156.977 MHz となった．回路は FPGA デバイスのおよそ 13%と小型であり，廉価な FPGA にも実装可能なハードウェア規模に抑えられている．

表 1 に試作した試験装置の主な性能をあげる．装置は 156.25 MHz で動作させており，フレーム間ギャップやガードタイムの調整幅は 6.4 ns となっている．問題が発生した際の原因となるトラフィックパターンを高精度で抽出することにより，回路シミュレータ上で問題を再現可能としている．最小ギャップ時間は Ethernet 規格の 9.6 ns に対し 12.8 ns に制限されている．すなわち，本装置は最小フレーム長 64 byte の場合，ワイヤスピードの約 95.5%のスループットとなる．したがって，ネットワーク装置評価である RFC2544 などには対応しておらず，厳密なスループットなどの性能評価には既存の専用試験装置を用いる必要がある．この制限は，最小フレーム長の 64 byte のフレームをフレームテーブルから読み出す際に 11 サイクルかかり，回路の内部バスが 8 byte 幅であることから生じている．つまり，プリアンブルをあわせて 9 サイクルで送出できるフレームの読み出しに 11 サイクルかかるため，フレーム間隔ギャップは 2 サイクル必須であり，$6.4 \times 2 = 12.8$ ns が最小となっている．以下，本装置で測定できる最大のスループットを最大転送速度と呼ぶ．**図 6** に本装置のフレーム長に対する最大スループットを示す．

ハッシュテーブルのエントリ数はトラフィックに含まれるフレームの種類の最大数であり，多いほど複雑なトラフィックを生成可能であるが，一方，テーブルの検査時間が比例して増加するためトレードオフをとる必要がある．本実装では，フレームテーブルのエントリ数が 65536 であり，このときの検査時間が約 419.4 μs とミリ秒以下に抑えられていることから，65536 エントリとした．

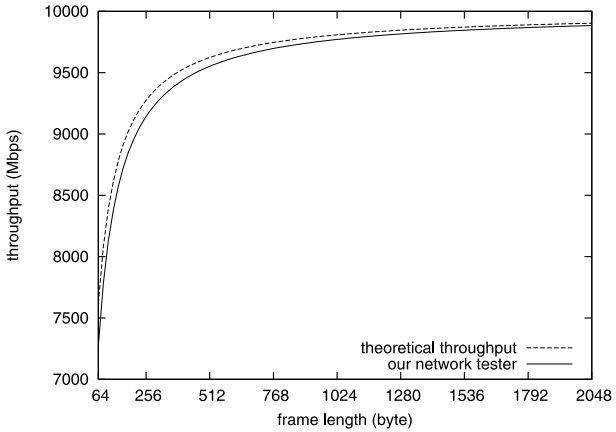

図 6　試作した試験装置のスループット
Fig. 6　Throughput of our network tester.

本装置はあらかじめ定めた転送速度のトラフィックに対して試験対象の機能と性能が満たされているかを 1 回の試験で評価できるが，これを応用して以下の手順により複数の試験を行ってフィルタリング装置の最大性能を測定することが可能である．

(1) ギャップ長を $n = 0, 1, ..., 22$ の順に 6.4×2^n ns と設定して試験を行い，転送エラーが起こらない最小の n を探す．n が見つかれば手順 (2) に進む．見つからない場合は $n = 23$ とする．
(2) 転送エラーの起こらない最小ギャップ長 $6.4\,m$ ns を探す．m の 2 進数表記を $[b_{23}b_{22}...b_1b_0]$ とし，初期値を 0 とする．まず，$b_n = 1$ を設定して試験を行い，転送エラーが起こらなければ $b_n = 0$，エラーの場合は $b_n = 1$ に固定する．次に $b_{n-1} = 1$ を設定して同様の試験を行う．これを b_0 まで順に繰り返す．
(3) 手順 (2) で定まった $6.4\,m$ ns でギャップ長を設定して試験を行い，転送エラーが生じた場合は m に 1 加算する．$m = [11...11]$ の場合で転送エラーが生じたときは，ハッシュテーブルのダンプを行い，正しく転送できたフレームの個数からスループットを参考値として出力して終了する．

© 2008 Information Processing Society of Japan

(4) 以上の $2n+1$ 回の試験により，転送エラーが起こらない場合の最小ギャップが分かる．試験で使用したトラフィックの平均フレーム長を l とすると，スループットは $\frac{l}{8+l+8m} \times 10 \times 10^3$ Mbps で算出できる．

性能測定で使用するトラフィックは制御 PC により様々なパターンとすることが可能である．本実装においては，指定した形式のトラフィックを生成し，試験対象の最大スループットを自動的に測定するツールを開発した．

4. 試作装置による試験の実施

フィルタリング装置のプロトタイプ開発の目的は，アルゴリズムや装置構成が期待した性能を発揮できるかどうか，また，正しく機能するかどうかを評価することである．本章では，試験装置を用いて 2 つのプロトタイプ装置，URL フィルタリング装置と IPS 装置それぞれの性能評価と機能試験を行った．

プロトタイプ装置の開発では，アルゴリズムの問題だけでなく設計ミスによる不具合が多数発生し，修正に多くの工数を費やしてしまう．そこで，プロトタイプ装置を開発する早期の段階で試験装置を用いて修正工数の短縮を図った．その結果，試験装置によってプロトタイプ装置で発生した不具合の原因となるトラフィックパターンを即座に絞り込むことが可能であることが分かった．これはトラフィックを制御 PC で詳細に調整し，ハッシュテーブルのダンプをフレームテーブルと照らし合わせることによって不具合の原因となるフレームを判断することができたためである．そして，制御 PC のツールでトラフィックをファイルへ出力し，論理シミュレータ上で同じトラフィックを再現しつつ回路のどの個所が問題となっているか迅速に検証することができた．試験時間は数分程度であり，回路シミュレータにおける問題再現におよそ 1〜2 時間，原因個所の特定と修正に数時間程度要している．さらに，トラフィックを試験装置で再現して，不具合が正しく修正されているかをプロトタイプ装置上で検証することができ，一連の修正が加速されたのである．

以下，URL フィルタリング装置と IPS 装置それぞれの試験について詳細を述べる．

4.1 URL フィルタリング装置

URL フィルタリング装置は HTTP リクエスト中の URL をデータベースと比較し，一致した場合にリクエストを遮断して有害なコンテンツへのアクセスを防ぐものである．試験対象であるプロトタイプ装置は，論文 9) の手法により構成されており，ネットワークに対して透過的に接続されている．プロトタイプ装置の概要を**図 7** に示す．初期段階のプロトタイプ装置は 10 Gigabit Ethernet インタフェースを持つが，Infiniband ×1 ポートが最大

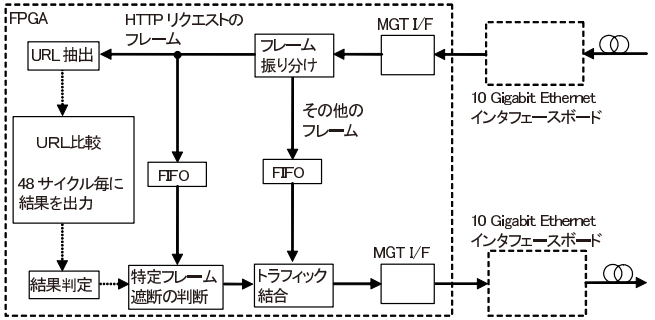

図 7　試作した URL フィルタリング装置の概要
Fig. 7　Conceptual diagram of the URL filtering system.

2.0 Gbps のスループットである環境に実装しており，動作周波数は 100 MHz，最大スループットは 6.4 Gbps となっている．

まず URL フィルタリングと関連のない ICMP フレームのみで構成されたトラフィックを用いてフィルタリングを行っていない場合の最大スループットを計測した．フレーム長を 64 byte 間隔で 64〜2048 byte に変化させて計測した結果，すべてのフレーム長で最大転送速度（6.4 Gbps 時）となることを確認した．フレーム長の変更は制御 PC 上で自動的に行っており，試験時間は数分程度要した．

次に，1024 個の HTTP リクエストフレームを無作為に組み合わせて構成したトラフィックを用いて機能評価と性能評価を行った．リクエストフレームの平均長は 272 byte である．試験の結果，フレーム間のギャップが 130 ns 以上であればフレームの欠落なくフィルタリングが正しく機能することが分かった[10]．さらに，HTTP リクエストフレームにダミーのランダムデータを付加し，フレームの平均長を 998 byte と 1505 byte として試験を行ったところ，最小のフレーム間ギャップはいずれも 110 ns となった．

以上の結果より，HTTP リクエストを扱う回路にボトルネックが存在し，さらに，あるフレーム長以下では URL をデータベースと比較する個所にボトルネックがあると推定される．プロトタイプ装置の設計では，1 回の URL の比較あたり 48 サイクルの処理時間となっている．回路の処理データ幅は 8 byte であるから，先ほどの試験で用いたフレームの平均長 272 byte は 34 サイクルに相当し，フレーム長のギャップ 130 ns は 13 サイクル，フレームのプリアンブルが 1 サイクルに相当することを考えると，$34+13+1=48$ サイクルであり，これが URL の比較時間と一致するためである．すなわち，装置の性能を向上させる

© 2008 Information Processing Society of Japan

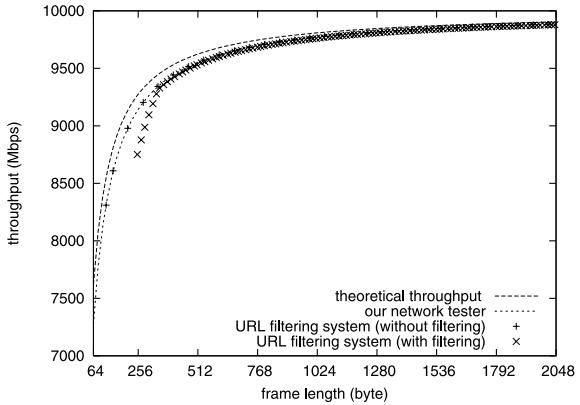

図 8　URL フィルタリングシステムの最大スループット測定結果
Fig. 8　Maximum throughput of the URL filtering system.

には HTTP リクエストを扱う回路の改善が必要であり，さらに，短いフレーム長のリクエストに対して URL の比較回路を修正すべきであると推測できた．

このような性能改善点が推定できたほか，プロトタイプ装置の処理能力を超えた高負荷を与えたとき，フレームを HTTP リクエストとその他に分類する回路や HTTP リクエストから URL を抽出する回路のシーケンサが異常な状態となり，装置の処理が停止してしまう不具合を発見・修正することができた．

得られた改善点に従って，URL 抽出を行う回路や比較回路を修正し，最大スループットが 10 Gbps の環境に実験的な回路の実装を行った．このプロトタイプ装置に対して，HTTP リクエストを含まないフレームにより測定した場合の最大スループットと，HTTP リクエストフレームを最小 252 byte から 16 byte ずつ変化させて性能測定を行った結果を**図 8** に示す．図 8 中の URL filtering system（without filtering）は HTTP リクエストを含まないフレームによる測定結果であり，URL filtering system（with filtering）は HTTP リクエストを含むフレームを用いた測定の結果となっている．なお，フィルタリング対象である HTTP リクエストフレームが含まれる割合を変化させてもスループットは変化しなかった．

平均フレーム長が約 350 byte 以上では，HTTP リクエストフレームを扱う回路の高速化により最小ギャップが 19.2 ns と大幅に改善し，ほぼ最大転送速度を達成可能であることが示された．一方，小さなフレームでは，フレーム長とプリアンブル，ギャップ長の合計がおよそ 288 ns となるように最小ギャップ長が増加し，スループットが低下している．このような結果より，さらに高い性能を得るには HTTP リクエストフレームの処理のサイクル数を低減させることが必要であると考えられる．

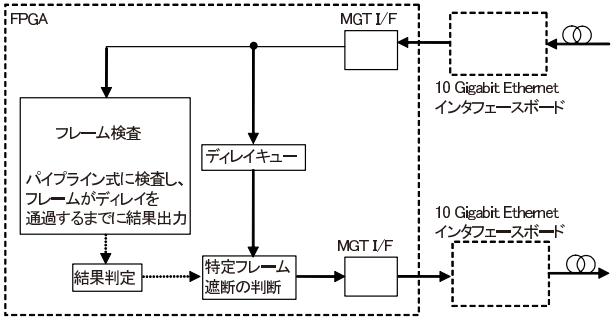

図 9　試作した IPS の概要
Fig. 9　Conceptual diagram of the IPS.

以上の URL フィルタリング装置の試験では，試験トラフィックの高い調整精度により改善点を抽出することが可能となった．また，不具合の原因を特定する際に，1〜2 時間程度要するシミュレーションの代わりに数分の試験をトラフィックを変化させつつ繰り返すことで原因の絞り込みを行うことができた．

4.2　IPS

IPS はトラフィック中の特定のフレームを遮断することにより，ネットワークシステムを侵入や攻撃から保護するシステムである．試験対象である IPS は，過去の侵入や攻撃より得られた検知パターンによりフレームを判別するシグネチャ方式であり，ネットワークに対して透過的に接続される構成となっている．IPS のプロトタイプ装置は論文 11)，12) の手法により構成されており，ソフトウェアベースの IDS である Snort [13] のルール中の 1225 個に対応する回路が試験装置と同様の環境に実装されている．プロトタイプ装置の概要を**図 9** に示す．

まず，検知パターンに該当しない ICMP フレームにより構成されたトラッフィックを用いてフィルタリングを行っていない場合のスループットをフレーム長を 64〜2048 byte 間で 64 byte ずつ変化させて計測し，すべてのフレーム長で最大転送速度となることを確認した．そして，プロトタイプで検知する 1225 個のルールから擬似的な攻撃・侵入トラフィックを生成し，フィルタリングが行われている場合のスループットを計測した．検知ルールに該当するデータのみで構成されたフレームに 64 byte ずつダミーのランダムデータを付加してフ

© 2008 Information Processing Society of Japan

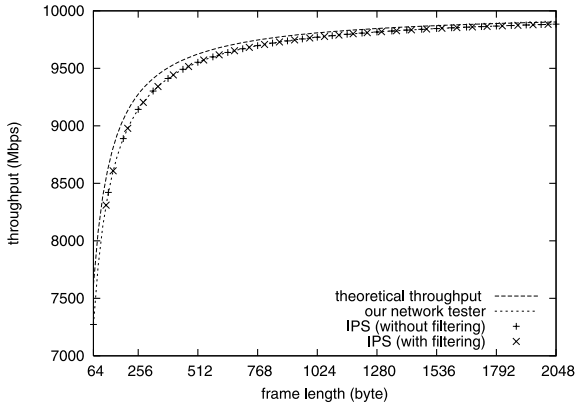

図 10　IPS の最大スループット測定結果
Fig. 10　Maximum throughput of the IPS.

レーム長を変化させて計測したところ，フィルタリングが行われる場合においても最大転送速度となることが分かった．**図 10** に測定結果を示す．フレーム長の変更は URL フィルタリングの試験と同様に制御 PC 上で自動的に行っており，試験時間は数分程度要した．

IPS のプトロタイプ装置では，あらゆるフレームを一定時間の間にパイプラインで検査する構成となっており，検知ルールに該当するかどうかが処理性能に影響しない構成としたが，試験結果より設計どおりに機能していることが確認できた．

次に，プロトタイプ装置が展示などのデモンストレーションに使用される場合を想定して，長時間にわたる試験を実施し信頼性の評価を行った．試験では攻撃の種類や割合が異なる 4 つトラフィックを用意し，これを数百ミリ秒〜数十秒の任意の時間で切り替えつつ断続的に負荷を与え続けた．トラフィックの切替えごとにハッシュテーブルを検証し，その結果を制御 PC へ通知してから次のトラフィックの設定を変更しており，数百ミリ秒程度の間隔を持った断続的な試験となっている．トラフィックの設定ではギャップ長やフレームテーブルの参照アドレスなどを無作為に変化させ，様々なトラフィックを擬似的に生成させている．転送エラーが発生した際はただちに試験を停止し，ハッシュテーブルをダンプして報告を行う．長時間にわたる試験を行ったところ，8 時間以上の連続動作においても転送エラーは発生せず，数時間のデモンストレーションの使用に十分な信頼性を持つことを確認することができた．

以上の IPS 装置の試験では，装置が設計どおりに機能し 10 Gigabit Ethernet の最大転送速度で動作可能であることを示したが，これは従来のネットワーク製品向けの専用装置でも示すことができる．しかし，プロトタイプ装置の完成度を高める際には，URL フィルタリング装置の場合と同様に数分の試験を繰り返すことで不具合の原因の絞り込みを行っており，本試験装置により検証期間を短縮することができた．また，性質の異なるトラフィックを切り替えた長時間にわたる負荷試験により，フィルタリングの性能をデモンストレーションすることがプロトタイプ装置で可能であることを確認することができた．

5. おわりに

本論文では，ハッシュテーブルを用いたフレーム判別の手法をハードウェア化することによりフィルタリング装置の機能試験を高速に行う手法を提案した．本手法ではトラフィック中のフレームが転送された個数のみがハッシュテーブルに記録され，フィルタリング装置の入出力に対応するテーブルが比較されることにより，フレームが正しく遮断もしくは転送されているかを評価している．この手法によりハッシュテーブルの比較時間を固定かつ短く抑えることが可能であり，高速な機能試験が実現できるようになった．

本手法により 10 Gigabit Ethernet に対応し，ネットワークフィルタリング装置の機能試験と性能評価を同時に実施する試験装置の実装を行った．そして，試験装置を URL フィルタリング装置や IPS 装置の開発における評価試験に利用し，その有効性を検証した．その結果，URL フィルタリング装置ではボトルネックとなっている原因を発見でき性能向上が可能となったほか，初期の開発において様々な不具合を迅速に修正することができた．一方の IPS 装置においても機能試験と性能評価によりアルゴリズムや構成の効果を確認でき，長時間にわたる負荷試験の実施によって，プロトタイプ装置の信頼性を検証することができた．以上の検証において，試験装置が機能や性能の検証だけでなく，改善点や不具合の修正点の発見に有効であることを示した．

謝辞　本研究は，平成 19 年度総務省戦略的情報通信研究開発推進制度（SCOPE）の委託研究「超高速ネットワークに対応した悪意ある通信の遮断技術の研究開発（課題番号：072003008）」の一環として実施されたものである．

参 考 文 献

1) Force 10 Networks P-series, Motel P10 Intrusion Prevention System Performance Evaluation, Technical Report 206126, THE TOLLY GROUP (2006).
2) Lippmann, R.P., Fried, D.J., Graf, I., Haines, J.W., Kendall, K.R., McClung, D.,

© 2008 Information Processing Society of Japan

Weber, D., Webster, S.E., Wyschogrod, D., Cunningham, R.K. and Zissman, M.A.: Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation, *Proc. 2000 DARPA Information Survivability Conference and Exposition, 2000*, Vol.2 (2000).
3) Cope, J., Voran, T., Woitaszek, M., Boggs, A., McCreary, S., Oberg, M. and Tufo, H.M.: Experiences Deploying a 10 Gigabit Ethernet Computing Environment to Support Regional Computational Science, *the 8th LCI International Conference on Linux Clusters: The HPC Revolution* (2007).
4) Seamans, E. and Alexander, T.: Chapter 35: Fast Virus Signature Matching on the GPU, *GPU Gems 3*, Addison Wesley Professional, pp.771–783 (2007).
5) HITACHI Inc: *Hitachi Ultrastar^{TM}15K300*.
6) 太田　聡：ハッシュ関数を用いた IP ネットワークのパッシブ遅延変動測定法における記憶領域削減と測定誤りの回避，電子情報通信学会論文誌，Vol.J89-B, No.1, pp.10–21 (2006).
7) Xilinx Inc.: *Virtex-II Pro and Virtex-II Pro X Platform FPGAs: Complete Data Sheet, DS083* (2007).
8) 片下敏宏，坂巻佳壽美，名古屋貢，寺島康典，戸田賢二：高速かつ軽量な可変データ長対応の CRC-32 回路構成手法，情報処理学会論文誌，Vol.48, No.7, pp.2382–2392 (2007).
9) 戸田賢二，片下敏宏，坂巻佳壽美，名古屋貢，寺島康典：高速ネットワークフィルタリング装置のアーキテクチャ，信学技報，Vol.106, No.290, pp.19–23 (2006).
10) 片下敏宏，坂巻佳壽美，乾　剛，高山匡正，名古屋貢，寺島康典，戸田賢二：ネットワークフィルタリング装置向け試験装置の評価，信学技報，Vol.105, No.671, pp.49–54 (2005).
11) Katashita, T., Maeda, A., Toda, K. and Yamaguchi, Y.: Highly Efficient String Matching Circuit for IDS with FPGA, *FCCM2006*, pp.285–286 (2006).
12) Katashita, T., Maeda, A., Toda, K. and Yamaguchi, Y.: A METHOD OF GENERATING HIGHLY EFFICIENT STRING MATCHING CIRCUIT FOR INTRUSION DETECTION, *FPL2006*, pp.799–802 (2006).
13) Roesch, M.: Snort - lightweight intrusion detection for networks, *13th Systems Administration Conference, LISA '99*, pp.229–238 (1999).

(平成 19 年 10 月 5 日受付)
(平成 20 年 3 月 4 日採録)

片下　敏宏

2006 年筑波大学大学院システム情報工学研究科修了．博士（工学）．現在，産業技術総合研究所情報技術研究部門特別研究員．主としてネットワークセキュリティ，回路設計に関する研究に従事．電子情報通信学会会員．

坂根　広史（正会員）

1990 年山口大学工学部電子工学科卒業．1992 年電気通信大学大学院電気通信学研究科博士前期課程電子工学専攻修了．同年通商産業省工業技術院電子技術総合研究所入所．2001 年独立行政法人産業技術総合研究所に組織変更．現在，同所主任研究員．同年電気通信大学大学院情報システム学研究科博士後期課程情報ネットワーク学専攻修了．博士（工学）．2002 年より 2005 年までデラウェア大学客員研究員．マルチコアアーキテクチャおよびそのエミュレーション方式，情報セキュリティを含む FPGA 応用，および暗号実装の安全性に関する研究に従事．電子情報通信学会会員．

堀　　洋平（正会員）

1999 年筑波大学第三学群工学システム学類卒業．2004 年同大学院博士課程修了．同年（独）産業技術総合研究所情報処理研究部門（現，情報技術研究部門）特別研究員．多目的映像表示装置，コンテンツ保護システム等の研究開発を行う．現在，FPGA の動的部分再構成を利用したリコンフィギャラブルシステム，暗号ハードウェアモジュールの耐タンパ性評価に関する研究に従事．電子情報通信学会会員．博士（工学）．

© 2008 Information Processing Society of Japan

戸田　賢二（正会員）

1982 年慶應義塾大学大学院工学研究科修士課程修了．同年電子技術総合研究所入所．以来，並列コンピュータのアーキテクチャの研究に従事し，記号処理用データ駆動計算機や実時間処理用並列計算機の開発を行った．近年は組み込み応用をターゲットとし，開発環境の整備とともに実時間処理用ハードウェアやネットワークの実用化研究を推進中．

© 2008 Information Processing Society of Japan