社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－SLDM－124 (9)
2006／3／16

ネットワークフィルタリング装置向け試験装置の評価

片下 敏宏[1] 坂巻 佳壽美[2] 乾 剛[2] 高山 匡正[2] 名古屋 貢[3] 寺島 康典[4] 戸田 賢二[1]

1) 産業技術総合研究所 〒305-8568 茨城県つくば市梅園 1-1-1 中央第2
2) 東京都立産業技術研究所 〒115-8586 東京都北区西が丘 3-13-10
3) デュアキシズ(株) 〒100-6014 東京都千代田区霞ヶ関 3-2-5 霞ヶ関ビル 14 階
4) (株)ビッツ 〒141-0031 東京都品川区西五反田 8-8-20 ダーバン本社ビル 8F

E-mail:1){t-katashita, k-toda}@aist.go.jp,2){sakamaki.kazumi, takayama.tadamasa, inui.takeshi}@iri.metro.tokyo.jp, 3)mnago@duaxes.co.jp, 4) terashima@bits.co.jp

あらまし 近年ではネットワークセキュリティシステムが必須となっており，その1つとしてネットワークフィルタリング装置が挙げられる．ネットワークフィルタリング装置は用途に応じてファイアウォールや迷惑メールフィルタ，コンテンツフィルタリング，URL フィルタリングなど様々なものが研究開発されている．これら装置の研究開発では機能試験やスループット測定などの評価試験が必要であり，我々はこれら試験を実施するための試験手法を提案している．本試験手法はハッシュテーブルを用いた送受信パケットの検査方式を用いており，試験装置の軽量な実装が可能であるという特長を持つ．本研究では先行研究で行った試験装置の試作で得られた改善点を元に試験装置の構成を改良し，さらに 10 Gigabit Ethernet のインタフェースに対応し最大 6.4 Gbps のスループットを持つ試験装置の試作を行った．そして，URL フィルタリング装置の開発において本試作試験装置により機能試験やスループット測定の評価を行った．

キーワード パケットフィルタリング，ネットワークセキュリティ，FPGA

Verification of Experimental Evaluation System for Network Filtering Systems

Toshihiro Katashita[1] Kazumi Sakamaki[2] Takeshi Inui[2] Mitsugu Nagoya[3] Yasunori Terashima[4] and Kenji Toda[1]

1) National Institute of Advanced Industrial Science and Technology
Tsukuba Central 2, 1-1-1 Umezono, Tsukuba-shi, Ibaraki 305-8568, Janan
2) Tokyo Metropolitan Industrial Technology Research Institute 3-13-10 Nishigaoka, Kita-ku, Tokyo 115-8586, Japan
3) DUAXES Corporation, Kasumigaseki Bldg., 3-2-5 Kasumigaseki, Chiyoda-ku, Tokyo 100-6014, Japan
4) BITS Co., Ltd., D'urban Bldg., 8-8-20 Nishi-gotanda, Shinagawa-ku, Tokyo 141-0031, Japan

E-mail: 1) {t-katashita, k-toda}@aist.go.jp, 2){sakamaki.kazumi, takayama.tadamasa, inui.takeshi}@iri.metro.tokyo.jp, 3)mnago@duaxes.co.jp, 4)terashima@bits.co.jp

Abstract. The network security system is necessary for our society in recent years, and network filtering systems have been studied such as the firewall, the spam mail filter, the contents filtering, and URL filtering. We proposed an evaluation system for the network filtering systems. Evaluating network systems using the hash table, the evaluation system does not need large memory resources. In this paper, we improved our evaluation system composition from the preliminary system in the previous our study, and made an experimental evaluation system for the 10 Gigabit Ethernet with up to 6.4 Gbps throughput. We evaluated a throughput measurement and a function examination of an URL filtering system.

Keyword URL filtering, network security, FPGA

1. はじめに

コンピュータネットワークによるサービスが我々の社会に広まる一方，利用者の増加などによりネットワークサービスに対する攻撃や侵入，不正な情報の流出，コンピュータウィルスの感染，有害な情報の氾濫などの問題が顕在するようになった．そのため，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．このネットワークセキュリティの方策として，ネットワークのパケットをある条件に従って遮断し，不正な情報の伝達などを防ぐフィルタリングが研究されている[1]．

このようなフィルタリング装置の研究開発におい

ては，試作装置の機能試験やスループットの測定によりアルゴリズムや装置構成の有効性を検証する必要性がある．フィルタリング機能やネットワーク装置としての機能は，装置に入力するパケットと出力されるパケットを比較することにより評価できる．しかし，単純に入出力されたパケットを記録し比較を行う手法では，巨大な記憶領域が必要となるほか，入出力パケットの比較に多くの時間を要するという問題がある．また，パケットの順番が装置通過時に入れ替わる場合への対処が必要となる．

そこで我々は，ハッシュテーブルを用いて入出力パケットの比較を行う軽量なフィルタリング装置の試験手法を提案している[2]．本手法は入出力パケットからハッシュ値を算出し，その値の指すテーブルの値を加算してパケットの種別のみを記録する．そして，入出力それぞれのパケットから生成したハッシュテーブルを比較することにより評価を行う．このため，必要な記憶領域はハッシュテーブルを格納する小規模なものとなる．また，テーブルの比較時間は固定であり，高速な評価が可能となる．

研究[2]では提案手法を 2 つの FPGA へ実装し 1 Gigabit Ethernet 用の試験装置を試作したところ，多くの改善すべき点が明らかになった．そこで本研究では試験装置の構成を改善し，さらに，10 Gigabit Ethernet のインタフェースに対応する試験装置の試作を行った．

そして，URL フィルタリング開発において試作 URL フィルタリング装置の機能試験やスループット測定を本試作装置によって評価した．この評価により URL フィルタリング装置の不具合やボトルネックとなっている箇所を発見することができた．

本論文では，まず提案しているネットワークフィルタリング装置の試験手法について述べる．次に研究[2]の試作から得られた試験装置の構成の改善点と 10 Gigabit Ethernet インタフェースに対応する装置の試作について述べる．最後に，試験装置の評価を行う．

2. フィルタリング装置と試験装置

ネットワークを通過するパケットを特定の条件に従って遮断し不正な情報の伝達などを防ぐセキュリティ技術がフィルタリングであり，用途に応じて様々な装置が研究開発されている．パケットのヘッダ情報を元に不正なアクセスを遮断するファイアウォールのパケットフィルタリング，特定のキーワードや送信元アドレスを元に迷惑メールや情報漏洩メールを削除するメールフィルタリング，特定の URL へのアクセスを防止し有害なコンテンツや業務と関連のないコンテンツにアクセスさせない URL フィルタリング等が挙げられる．

このようなフィルタリング装置を研究・開発する際には，装置の機能試験やスループット測定によりアルゴリズムや装置構成の有効性を検証する必要がある．この検証を行う装置がネットワーク試験装置である．

2.1. フィルタリング装置の試験装置

フィルタリング装置の評価における試験項目として，フィルタリング機能，ネットワーク装置としての機能，スループットが挙げられる．

1) フィルタリング機能

決められたパケットのみが遮断され，その他のパケットは通過することを確認し，フィルタリングが正しく機能しているか評価する．

遮断対象パケットとそうでないパケットが混在したトラフィックをフィルタリング装置へ入力し，装置からの出力されたトラフィックを比較する試験方法が考えられる．

2) ネットワーク装置としての機能

異常な形式のパケットが入力された場合でも装置は動作可能であるかなど，フィルタリング装置がネットワーク装置として正しく動作するか評価する．

様々なパケットが混在したトラフィックをフィルタリング装置へ入力し，装置の状態や出力されるトラフィックを確認する試験方法が挙げられる．

3) スループット

フィルタリング装置のスループットを測定する．

パケットの遮断が行われる際のスループット測定は，フィルタリング装置がパケットを欠落せず処理できるトラフィックのスループットを測定する方法が考えられる．このとき，短いトラフィックを用いるとフィルタリング装置のバッファなどで蓄積されてしまう可能性があるため，スループット測定では長いトラフィックを用いる．

このようにフィルタリング装置の評価は，試験対象装置に入力するパケットと装置から出力されたパケットを比較することにより行うことができる．しかし，入出力されるパケット全てを記録して比較を行うような手法をとると巨大な記憶領域が必要となる．また，パケットの順番が装置通過時に入れ替わる場合に対処する必要がある．さらに，送受信パケットの比較に多くの時間を要すると考えられる．

そこで我々は，ハッシュテーブルを用いて入出力パケットを比較することにより処理を軽量化する試験手法を提案している．

提案する試験手法の概要を図 1 に示す．試験装置は送信器と受信器の組から構成され，以下に示す手順で送受信パケットを比較することによりフィルタリング機能の試験を行う．

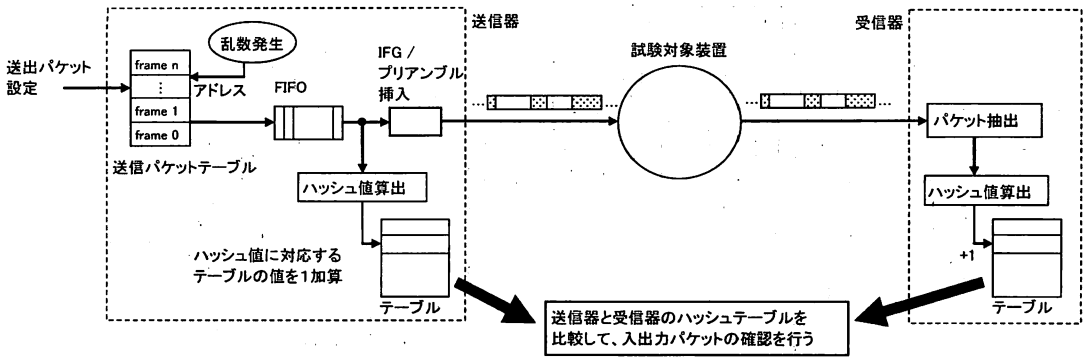

図 1： 提案する試験手法の概要

まず，試験で使用するパケットをあらかじめ生成し，送信器に設定する．このパケットをランダムまたは一定の法則に従って選択し FIFO へ入力する．そして FIFO からパケットを順次取り出し，指定された間隔の IFG（Inter Frame Gap）とプリアンブルを追加して試験対象装置へ入力する．このとき，FIFO から取り出したパケットからハッシュ値を算出し，ハッシュテーブルの値を 1 加算する．

次に，試験対象装置から出力されたトラフィックを受信器へ入力し，パケットの抽出を行って送信器と同様にハッシュ値の算出とテーブルの更新を行う．

最後に送信器と受信器のハッシュテーブルを比較することで，入出力パケットが一致しているかを確認する．ハッシュテーブルの値が異なる場合，異なっているテーブルのハッシュ値より異常が発生したフレームを特定することができる．

パケット間のハッシュ値の衝突は，パケット生成時にハッシュ値を計算し衝突があるパケットは IP パケットの ACK 値など機能評価に影響が無いと判断されるフィールドを変更し，あらかじめ回避しておく．

送信器に設定するパケットには，パケット長やフィルタリング装置で遮断されるかどうかを示すフラグをヘッダとして付加する．送信器でハッシュ値を計算する際，このヘッダ情報からフレームがフィルタリング装置で遮断されるかを判断し，遮断されるべきパケットからはハッシュ値を算出しない．このようにしてフィルタリング機能によりパケットが遮断される場合でも送信器と受信器のハッシュテーブルを対応させる．なお，パケットのヘッダは，送信時には削除する．

2.2. 試験装置の試作

研究[2]では提案する手法を用いて 1 Gigabit Ethernet 用のフィルタリング試験装置を試作した．実装は FPGA ボード REX[3]に 1 Gigabit Ethernet の PHY チップを接続した環境で行った．

本研究では，この試作により得られた以下の改善点を元に試験装置の構成を改良した．

- テスト開始・終了通知の改善
  試作では ARP パケットにより試験の開始と終了を通知していたが，この ARP パケットが欠落すると試験が正しく行えないという問題があった．そこで送信器と受信器を 1 つの FPGA に実装し内部信号で通知することにより問題を解決した．
- ハッシュテーブル収集・検査の自動化
  ホスト PC にハッシュテーブルを一旦収集してホスト PC 上で検査を行っていたが，FPGA でハッシュテーブルの収集・検査を自動的に行い，結果のみをホスト PC に通知する回路を追加した．
- ハッシュテーブルの 2 重化
  ハッシュテーブルの更新と収集を同時に行える様に 2 重化した．そして，前項のハッシュテーブル収集・検査の自動化と組み合わせることにより，長時間の連続的な試験を可能とした．
- スループット測定回路の付加
  IFG を自動的に調整しながら検査対象装置の最大スループットを計測するシーケンサを追加した．
- ハッシュ値算出の改善
  試作では排他的論理和によるハッシュ値の生成を行っており，ハッシュ値の衝突が起こり易い問題があった．そこでハッシュ値算出アルゴリズムに CRC-32 回路[4]を用いた．なお，パケット中の FCS はハッシュ値算出に含めない．
- フレームデータのランダム選択の実装
  試作ではシーケンシャルにフレームデータを選択しているが，これを CRC-32 による擬似乱数を用いて選択できる機能を追加した．

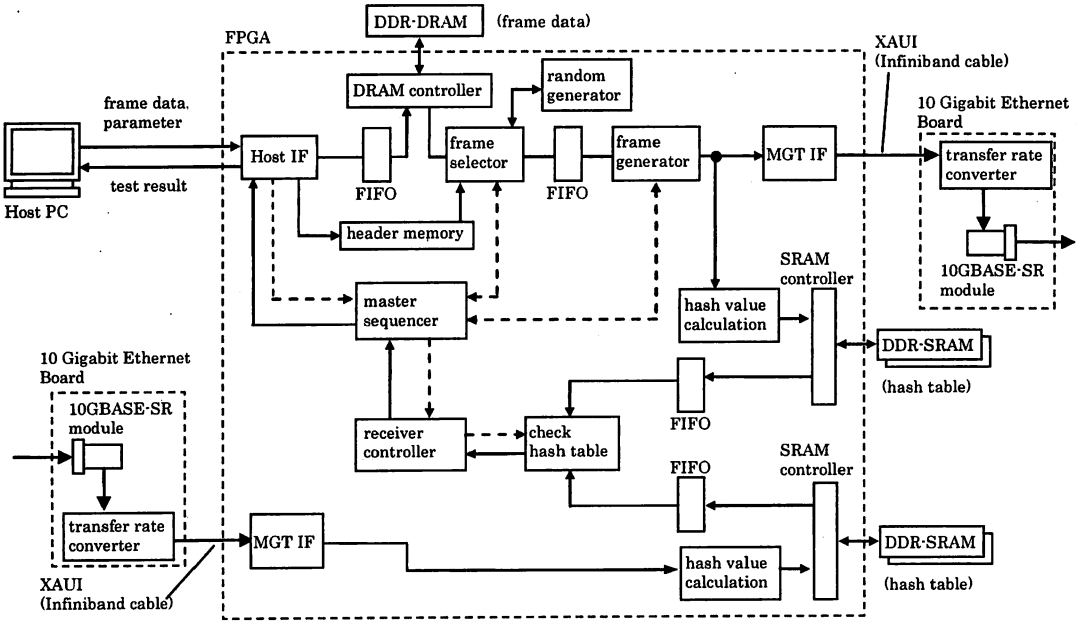

図 2：試験機のブロック図

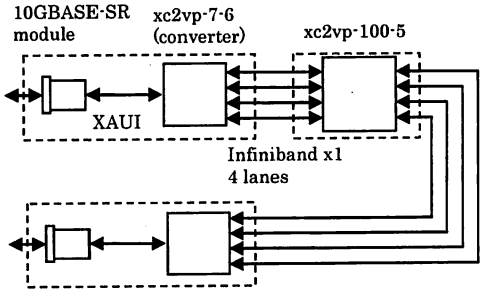

図 3：試験機の接続図

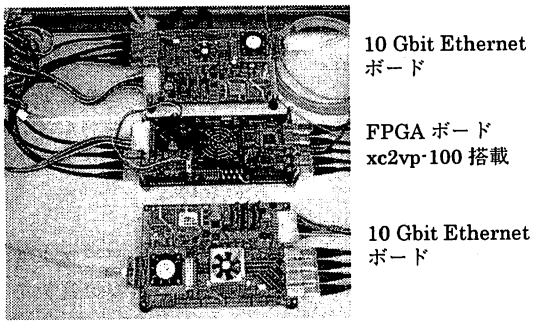

図 4：試験機の写真

そして，10 Gigabit Ethernet のインタフェースに対応したフィルタリング試験装置を試作した．実装した送信器の構成を図 2 に示す．また，図 3,4 に試作機の接続図と写真を示す．

試作装置の 10 Gigabit Ethernet への対応においては 10GBASE-SR 光モジュールとのインタフェース XAUI (10 gigabit Attachment Unit Interface) [5]を 4 レーンの Infiniband x1 へ変換するレート変換インタフェースボードを FPGA ボードに接続した環境を用いる．XAUI は 32 bit 単位でデータの入出力を行うが，FPGA に接続されている外部メモリなどの動作周波数を考慮してデータを 64bit 毎に扱うこととした．このとき 10 Gbps を得るには動作周波数を 156.25 MHz とする必要がある．しかし，今回使用した FPGA Xilinx Virtex-II Pro xc2vp-100-5 [7]は Infiniband の最大スループットが 2.0 Gbps(データは 1.6 Gbps)であったため，回路の動作周波数を 100 MHz とし最大スループットが 6.4 Gbps の試作を行った．レート変換インタフェースボードは 10 Gbps から 6.4 Gbps の転送レート変換が可能であり，この機能を用いてパケットの入出力を行う．

試作した試験装置は，最大長 8 KB の送信パケットを最大 32768 個 DDR-SDRAM に格納し，最大約 42 億回連続してランダムに送信できる．パケット間の IFG は最小 16 B から最大 127 MB に設定できる．ハッシュテーブルは DDR-SRAM に格納され，試験終了時に自動的に収集・検査される．ハッシュテーブルは 2 重化されており，収集・検査中も試験を行うことが可能である．また，ある IFG を設定し一定数バイト毎に IFG

を調整しつつ試験を行い，試験対象装置の処理可能な最小 IFG 長を測定する機能を持つ．

試作回路ではデータの処理単位を 8 B としたため，最小 IFG が 16 B となり，パケットの先頭が 8B のアライメント毎となった．

試験装置の回路を Xilinx ISE6.3sp3 で論理合成した結果，回路規模は 4928 Slice，7007 LUT，5631 FF となり最大動作周波数は 123.6 MHz となった．

3. 試作装置の評価

試作した試験装置を用いて開発中の URL フィルタリング装置の評価を行い，試験装置の有用性を検証した．

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．

試験装置と同様の環境に実装した試作 URL フィルタリング装置に対し，まず ICMP パケットを入力してフィルタリング動作を行っていない場合のスループットを計測した．パケット長を 4096 B から 64 B に順次変化させて計測した結果，全てのパケット長でほぼ理想的なスループットとなることを確認した[1]．

次に，1024 個の URL から HTTP GET リクエストパケットを生成し，これを 10000 回送出して URL フィルタリング装置の評価を行った．生成したパケットの平均長は約 272 B である．この結果，IFG が 104 B (プリアンブルは 8 B)までパケットを全て処理できることが分かり，結果としてスループットは

$$\frac{272}{272+114+8}\times 6.4(Gbps) \cong 4.53(Gbps)$$

と約 4.5 Gbps であることが分かった．

このスループット測定の結果と ICMP パケットによる測定により，試作した URL フィルタリング装置のボトルネックは URL の比較を行うマッチング部であることが推定できる．フィルタリング装置の設計において，URL マッチング部の処理サイクルが 48 サイクルとしていたが，処理データ幅が 64 bit であるのでマッチング処理中に通過するデータ長は 384 B である．

つまり，処理データ幅が 64 bit で 48 サイクルに通過するデータ長 384 B と，試験パケット転送で繰り返されるデータ長 (パケット長)+(IFG) = (272+112) = 384 B と一致する．

このような理由から URL フィルタリング装置のスループット改善には，マッチング部の処理サイクルの改善が必要であると推定できる．

このほか試験において，フィルタリング装置で処理できない高負荷を与えると装置が停止する等のバグを発見することができ，高負荷時にはパケットが欠落するが装置は停止しないように改善することができた．

このように，試験装置によって URL フィルタリング装置の問題や改善の推定を行うことができ，本試験手法の有用性を示すことができた．

4. まとめ

本論文では，10 Gigabit Ethernet インタフェースに対応し最大 6.4 Gbps スループットを持つネットワークフィルタリング装置向けの試験装置の試作を行った．

本装置は既に提案したハッシュテーブルによる軽量なフィルタリング装置の試験手法を実装したものである．本手法は送受信パケットを直接比較することなく試験を行うため全てパケットを記録する記憶領域を必要とせず，かつ，高速な検証を行うことができる特長を持ち，フィルタリング装置の連続試験を可能とするものである．

そして試作した試験装置により開発中の URL フィルタリング装置の試験を行い，提案する試験手法の有用性を示した．

課題としては以下の装置構成の改善点が挙げられる．

- 回路の高速化による最大スループットの向上

  試作では回路の動作周波数を 100 MHz としていたが，これを 156.25 MHz に向上させ最大スループットを 10 Gbps に向上させる．Infiniband の速度は FPGA を xc2vp-100-6 に変更することで最大 3.125 Gbps に向上し 10 Gbps に対応できる．
- パケット送信方式の追加

  本装置では設定したパケットにプリアンブルと IFG を付加して送信する方式であるが，これに加え，プリアンブルや IFG をパケットにあらかじめ付加したストリームをメモリに蓄積し，これをそのまま送信できる機能を追加する．

  繰り返されるパケットのパターンがメモリ長に固定されるが，回路中で処理するデータ幅を 8B としたために理想的な最小 IFG の 12 B[6]や，10 Gigabit Ethernet における瞬間的な最小 IFG の 9 B で送出できなかった問題を改善する．
- ハッシュ値算出方式の改善

  試作装置では CRC-32 をハッシュ値算出に用いていたため，パケット全てから値を算出すると結果は全て同じ値となる．そのため FCS (Frame Check Sequence)はハッシュ値の算出に用いなかった．

  ハッシュ値と FCS を比較し，異なっている場合

[1] 最大スループットが 6.4 Gbps 環境時．試験装置の最小 IFG が理想的な最小 IFG 12 B でないため，“ほぼ理想的”としている．

はハッシュ値をビット反転するなど，FCS もハッシュ値の算出に加える改善を行う．

- 遮断パケット数の記録

  フィルタリング装置で遮断されるパケットからはハッシュ値を算出しないことで送信器と受信器のハッシュテーブルを一致させていたが，試験で遮断されるパケットが何個送出されたのか分からない問題がある．

  遮断されるパケットから算出されたハッシュ値の指すテーブルの更新方法やテーブル空間の２重化などにより，送信器と受信器のテーブルを一致させつつ送出パケット数を記録する．

- ハッシュ値算出フィールドのマスク

  本論文で検証した URL フィルタリング装置はネットワーク透過型であり，通過するパケットに変更しない．しかし，TTL フィールドなどを変更するフィルタリング装置もあり，ハッシュ値を算出で特定のフィールドはマスクする等の対応方法を考案する．

これらの改善を行うほか，試験装置の操作インタフェースの整備等を行うことにより製品化を目指したい．

追記：

本研究は，平成１６年度 地域新生コンソーシアム研究「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」の一環として実施されたものである．

文　献

[1] 片山 善治 監修，“IT セキュリティソリューション大全 下巻 IT セキュリティエンジニアリング”，フジ・テクノシステム，2004.

[2] 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.

[3] Yuetsu Kodama, Toshihiro Katashita, Kenji Sayano, “REX: A Reconfigurable Experimental System for Evaluating Parallel Computer Systems”, IEICE Transaction Information & Systems, Vol. E86-D, No.10, Oct. 2003.

[4] 片下敏宏，坂巻佳壽美，乾剛，名古屋貢，寺島康典，戸田賢二，“10 Gigabit Ethernet 用の軽量かつ高速な CRC-32 回路の実装”，信学技報 DC2005-19, pp. 19–23, 2005.

[5] 石田 修，瀬戸 康一郎 監修，“１０ギガビット Ethernet 教科書 (初版)”，IDG ジャパン，2002.

[6] 泉谷建司，“Ethernet”，ソフト・リサーチ・センター，1997

[7] Xilinx Inc, “Virtex-II Pro and Virtex-II Pro X Platform FPGAs: Complete Data Sheet”