キャンパスネットワークにおける Winny 検知手法の FPGA 実装

FPGA Implementation of Winny Detection in a Campus Networks

佐藤　友暁†，伊丸岡 修哉‡，深瀬　政秋†
Tomoaki Sato †, Syuya Imaruoka ‡, Masa-aki Fukase †

tsato@cc.hirosaki-u.ac.jp, h08gs403@stu.hirosaki-u.ac.jp, slfuka@eit.hirosaki-u.ac.jp

†弘前大学総合情報処理センター
‡弘前大学大学院理工学研究科

† C&C Systems Center, Hirosaki University
‡ Graduate School of Science and Technology, Hirosaki University

概要

キャンパスネットワークにおける Winny の利用は，ネットワークの帯域を消費し，研究，教育，業務に支障をきたすだけでなく，情報漏えいや著作権侵害といった問題を引き起こす．Winny 利用への対策として，ネットワーク機器で全パケットをシグネチャマッチングによってアプリケーションを特定し，ファイル交換ソフトウエアのパケットを停止させる方法が有効である．しかし Winny はパケットペイロードが暗号化されており，ネットワーク機器において暗号化パケットペイロードをエンコードすることは，通信の秘密の侵害になる．さらに，キャンパスネットワークで使用されている 1Gbps 以上の高速な回線に適用可能なネットワーク機器おいて，暗号化パケットペイロードのエンコード機能は，処理能力上実装されていない．本論文では，ネットワークカードにおいて，暗号化パケットペイロードをエンコードし，パケットのシグネチャマッチングによって Winny の利用を検知する手法を FPGA (Field Programmable Gate Array)に実装する．その実装された検知機能の低消費電力化のために，ウェーブパイプライン動作ファイアウォールユニットと連動させる. ゲートレベルシミュレーションの結果, ギガビットイーサネットに対応可能であることを明らかにする．

キーワード

ファイル交換ソフトウエア，Winny，FPGA，IDS，IPS，ファイアウォール，ウェーブパイプライン，低消費電力

1. はじめに

インターネットアクセス回線のブロードバンドとともに P2P (Peer-to-Peer) 型のファイル交換ソフトウエアが広く利用されている. ファイル交換ソフトウエアの利用は，様々なファイルを不特定多数のファイル交換ソフトウエアユーザと共有できる一方，著作権侵害の原因となっている. また大学内のキャンパスネットワークにおいては，

ネットワークの帯域を消費し，研究，教育，業務に支障をきたす原因である．

加えて，ファイル交換ソフトウエアを経由した情報流出が多発している．特に，Winny [1]と呼ばれるファイル交換ソフトウエアは, 日本においてユーザ数が一番多い．そのために，Winny を経由した情報流出による被害が特に相次いでいる．このためファイル交換ソフトウエアを利用させないことが不可欠である．

そのための対策として，ファイル交換ソフトウエアの利用検知ソフトウエアを各コンピュータにインストールし，ファイル交換ソフトのインストールおよび利用を監視する手法がある．しかしソフトウエアによる監視手法は, インストールされたコンピュータの CPU リソースが監視のために消費され，アプリケーションの干渉による障害リスクが高まる問題がある．加えて，管理者権限を有する場合，ユーザ側で監視ソフトウエアを容易にコントロールすることが可能である．

ネットワーク機器によるファイル交換ソフトウエアの利用検知は，サービスポートが固定されているファイル交換ソフトウエア，またはパケットペイロードにアプリケーション特有の特徴が含まれている場合は有効である[2]. しかし Winny のようにサービスポートが固定されず, パケットペイロードが暗号化されている場合には有効でない[3].

ネットワーク機器において暗号化パケットペイロードをエンコードすることは，通信の秘密の侵害になる．このため，IDS (Intrusion Detection System) や IPS (Intrusion Prevention System) において, 暗号化パケットペイロードのエンコード機能は実装されていない．さらに，キャンパスネットワークで使用される 1Gbps 以上の回線では, 処理能力上，解析用専用プロセッサ必要である．

このため, [3]は Winny を特定できるトラヒック特定方式を開発した. 未検知率は0.053-0.116 に抑えられており, 誤検知率は 10^{-4} に抑えられている．しかし 100%の検知率は達成されていない．このトラフィック特定方式をネットワーク機器に組み込み，Winny パケットの遮断に使用した場合, 誤作動および作動しないことが起こりえる．

本論文では，Winny パケットを 100%の検知率で検知することを実現するために，暗号化パケットペイロードのエンコード機能と Winny 特有の特徴を解析するシグネチャマッチングを FPGA に実装する．これはネットワークカードに実装されるため，通信の秘密の侵害に相当しない．ゲートレベルシミュレーションによって，ギガビットイーサネットに対応可能であることを明らかにする．さらに実装する機能をより低消費電力で稼働させるために，ウェーブパイプライン動作ファイアウォールユニットと組み合わせる手法を提案する．

2. Winny

Winny は金子勇氏によって開発されたファイル交換ソフトウエアである[1]. 純粋 P2P タイプのファイル交換ソフトウエアであり，検索効率と匿名性を高めるために以下の特徴を有する．

- 階層構造のノード
- 元ファイルやファイル情報は中継ノードにキャッシュされる．
- キャッシュファイルおよびノード間の中継は暗号化される．

インターネット掲示板を中心として, 2002 年頃から普及し始めた．

ハイブリッド P2P は中心となるサーバが動作しなくなるとネットワークが停止するが，純粋 P2P は形成されたネットワークを停止させることができない．Napstar や WinMX は著作権関係の訴訟の結果，サーバのサービスが停止された．しかし, Winny は 2004 年に開発者が逮捕された現在でも利用可能である．

Winny は以下の特徴によって現在においても，国内で広く使われている．

- NAT (Network Address Translation), Firewall, ルータなどの設定を変更せず，0 port ノードとしてネットワークへの参加を許可している．セキュリティに対する知識や技術がなくても利用でき，被害拡大の一因となっている．
- 国内で開発され, 利用者のほとんどが日本人であるため, 日本人向けのファイルが多く共有されている．そのためにウイルスの蔓延もほぼ国内に限られ, 世界的に見て脅威が低いため対策が遅れる傾向がある．
- 主に各ノードが保持するのは, ファイルそのものではなくファイル情報であるため, ノードに要求される通信速度や HDD 容量が少ない．

2.1. Winny による情報漏えい

Winny の共有フォルダにおかれているファイルは Winny ユーザ間で共有される．このため，個人情報や，機密情報等のファイルを Winny の共有フォルダにおいた場合，第三者にそれらのファイルが流出する．さらに，Antiny と呼ばれるコンピュータウイルスの出現によって，情報漏えいの事件が多発している．

Antiny は，Winny のようなファイル交換ソフトウエアを経由し侵入し，以下の影響を与える．

- Antiny はファイル交換ソフトウエアの共有ファイルに置かれる．Antiny のファイル名は，検索キーワ

ードのマッチする名前にされる．

- そのファイルは他のファイル交換ソフトウエアのユーザによってダウンロードされる．
- そのファイルをダウンロードしたユーザは，そのファイルを実行する．
- 実行後，そのユーザの使用しているデスクトップやマイドキュメントフォルダ内のファイルを，Winny の共有フォルダにコピーする．
- Winny 実行時に，デスクトップやマイドキュメントフォルダ内のファイルは他の Winny ユーザに流出する．

表 1 に Winny による情報漏えいの例を示す[3].

表 1 . Winny による情報漏えい

Date	Origin	Content
Jan., 2008	Sagara Village Office	Individual information on 187 persons
Dec., 2007	Japan Atomic Energy Agency	Operating Information
Dec., 2007	**** University Hospital	Patient information on 195 persons
	⋮	
Oct., 2007	Osaka Pref. Police Department	Individual information on 200 persons
	⋮	
Jun., 2007	Japan Ground Self-Defence Force	Military forces member information on 100 persons
	⋮	

2.2. キャンパスネットワークにおける Winny 対策

ファイル交換ソフトウエアの使用は，情報漏えいの原因屋や著作権を侵害するだけでなく，ネットワーク帯域を消費する原因である．また，学生であっても研究等において，機密情報を扱ったりしている．このため多くの大学では，キャンパスネットワークにおいて，ファイル交換ソフトウエアの使用を禁止している．しかし，大学においても，利用規則による禁止のみならず，何らかの物理的な対策が不可欠である．

その一方，キャンパスネットワークにおいては，学生が所有するノート PC を接続するための環境を構築し[4], そのノート PC を教育に活用している[5]．特に大学内で使用されている個人のパソコンに関しては，民間企業等と異なり，通信の秘密を侵害するような方法でファイル交換ソフトウエア対策を行うことができない．

3. 提案システム

従来の Winny 検知手法の問題点を解消し，キャンパスネットワークにおいて適用可能するために開発を行う Winny 検知システムを図 1 に示す．Winny 検知システムは，FPGA を搭載した NIC (Network Interface Card) で構成されている．図 1 は有線 LAN の場合であるが，無線 LAN への適用は，RJ-45 コネクタとイーサネットコントローラを無線 LAN コントローラに置き換えることで，対応可能である．

FPGA はファイアウォールユニットとファイル交換ソフトウエアのパケットを検知するための回路を有し，それぞれの処理を行う．容易に回路構成を変更することが可能であることが FPGA を使用する理由である．そのため，File Exchange Detecting Unit を他のファイル交換ソフトウエアへ対応することやファイル交換ソフトウエアのバージョンアップへの対応は容易である．

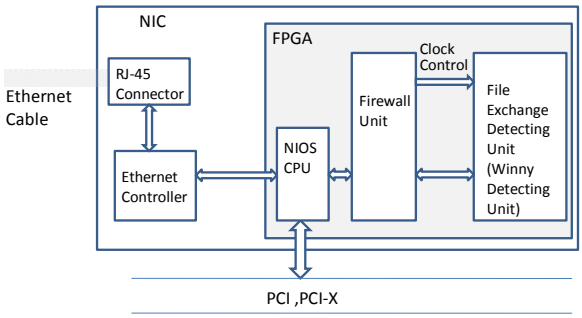

図 1 ． Winny 検知システム構成

3.1. Winny パケットの解析

Winny 検知ユニットのアルゴリズムを作成するために図 2 の Winny 解析用ネットワークを構築し，Winny パケットの解析を行う．10.0.50.3Winny 解析用ネットワークは，今後 Winny 検知システムの評価を行う際にも必要とされる．すでに，Winny のパケット解析は，[6]にて行われている．

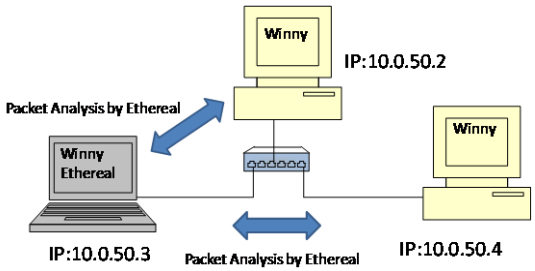

図２．Winny 解析用ネットワーク

しかし，[6]は商用のソフトウエアを使用しているため，我々はフリーソフトを使用した環境を構築する．ここで構築したネットワーク環境は，Winny 検知システムの評価に使用することも可能である．使用したソフトウエアは Etherreal である．Etherreal は IP アドレスが 10.0.50.3 に設定されている PC にインストールされている．図３に Etherreal による Winny パケットの解析結果を示す．

Winny のパケットは，RC4 (Rivest's Cipher 4)によって暗号化されている．RSA セキュリティ社の Ron Rivest によって開発された RC4 は，ストリーム暗号かつ共通鍵暗号方式である．無線 LAN において使用されている暗号である WEP (Wired Equivalent Privacy)においても，RC4 は使用されている．

図４は，Winny のキーパケットを Etherreal にて解析した結果である．キーパケットのデータ長は 11 バイトである．すべてのキーパケットは，暗号化データのデコードによって，01 00 00 00 61 というデコード結果を得ることができる．

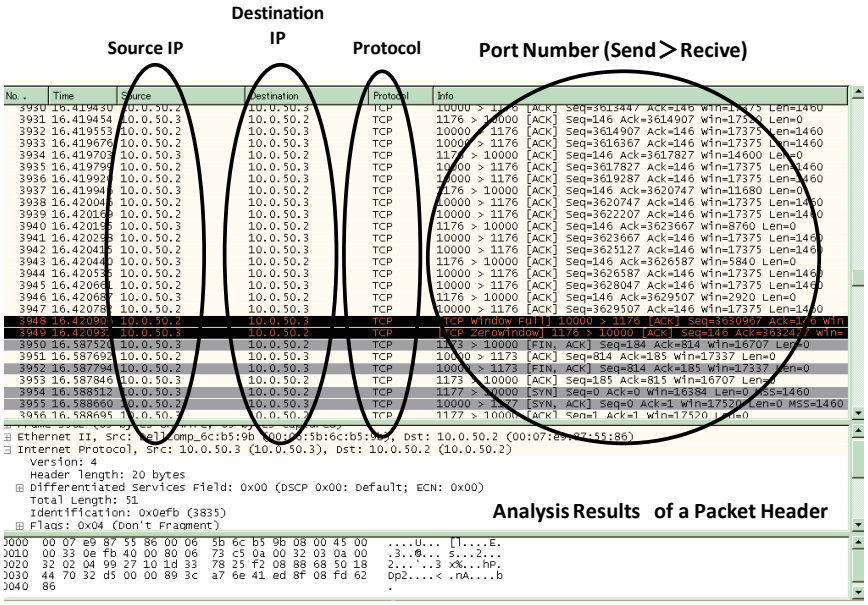

図 3. Winny パケット

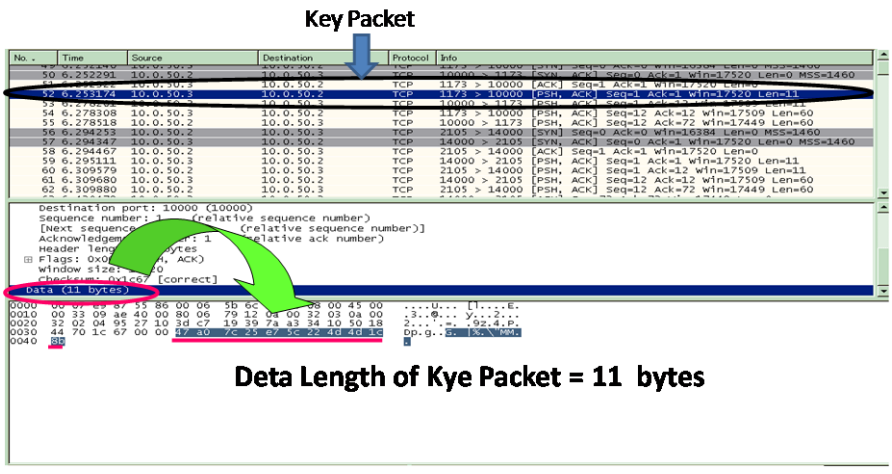

図４．Winny のキーパケット

3.2. Winny 検知ユニット

3.1 の解析結果をもとに, 我々は図５に示す検知アルゴリズムを提案する．検知方法は，最初にデータを読み込み，データ部が 11bytes なら AFD でデータ部の復号を行う．データ部の復号結果が鍵パケットの値と一致した場合，Winny と判定する．それ以外のパケットは Winny 以外の通信と判定する．

RC4 アルゴリズムは, RSA セキュリティ社によって公開されていない．このため，Arcfour という RC4 と互換性を有するアルゴリズムを使用する．図５の検知アルゴリズムは，表２の開発環境を使用して，FPGA へ実装される．

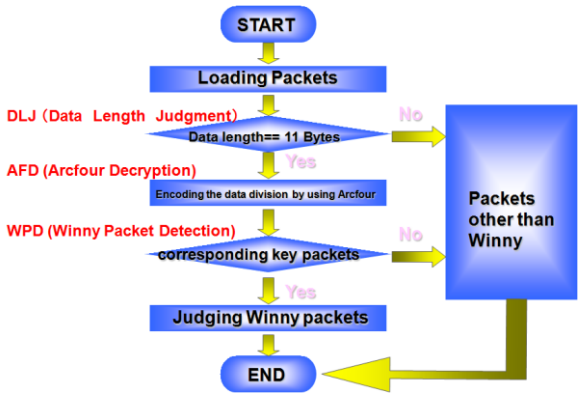

図５．Winny パケット検知アルゴリズム

表２．開発環境

OS	Microsoft Windows 2000
CPU	Intel Pentium III (1GHz)
Memory	256 MBytes
CAD	Altera QuartusII
FPGA Device	Altera Cyclone EP1C20F400C7

4. 評価

３章で実装した Winny 検知ユニットはロジックアナライザを使用し，FPGA を測定することで性能を評価できる．最初に，Winny 検知ユニットは論理合成ソフトウエアである Altera QuartusII によって FPGA 回路を合成される．図６はこの回路のゲートレベルシミュレーション結果である．次に，図６の結果をもとにロジックアナライザを使用して Winny 検知ユニット回路が書き込まれた FPGA を検証する．図７はロジックアナライザによって FPGA の信号を測定した結果である．

Winny 検知ユニットのスループット TP は次の式にて求めることが可能である．

$$TP = f \times W \times \frac{L_{Frame}}{L_{Data}} \quad (1)$$

ここでは，

f ：クロック周波数

W ：Winny 検知ユニットのワード幅 (bit)

L_{Frame} ： フレームのデータ長 (byte)

L_{Data} ：キーパケットのデータ長 (byte)

である．

Winny 検知ユニットは，図７の結果より 66MHz で動作することが確認される．また，ワード幅は 8 ビットである．イサーネットフレームは，

$$64 \le L_{Frame} \le 1518 \quad (2)$$

であるため，時間当たりの処理フレーム数が多くなるフレームの最小データ長を使用し，(1)式より，

$$TP = 3.072 \ \text{(Gbit / sec)} \quad (3)$$

が得られる．よってギガビットイーサネットへの対応が可能である．また，QuartusII によって得られた Winny 検知ユニットの消費電力は 214mW である．

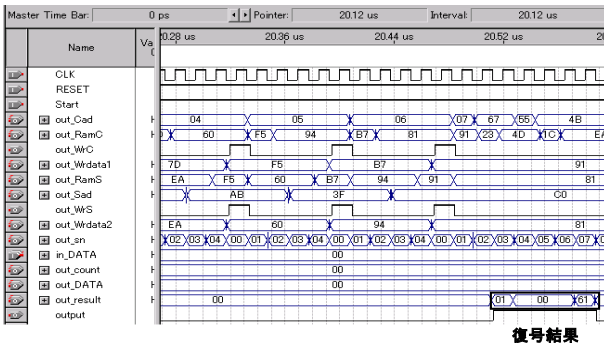

図６． ゲートレベルシミュレーション結果

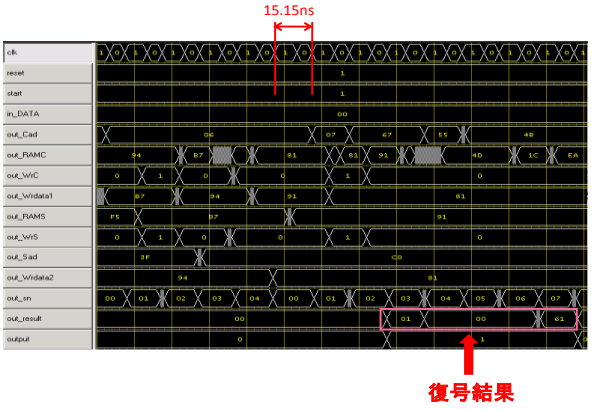

図７．測定結果

5. ウェーブパイプライン動作ファイアウォールユニット

Winny 検知ユニットは, バッテリで駆動するノートパソコンで使用することも考慮する必要がある．このため消費電力の削減が不可欠である．我々はさらなる消費電力の削減のために，ウェーブパイプライン動作ファイアウォール[7]を FPGA へ組み込み，このファイアウォールユニットから Winny 検知ユニットを動作させるためのクロックを制御する手法を提案する．

図８に表３のポートを制御する際のファイアウォールユニットを示す．ファイアウォールユニットは Winny 検知ユニットと同様に FPGA で実現されている. このため, 表３のポート番号の変更は容易である．

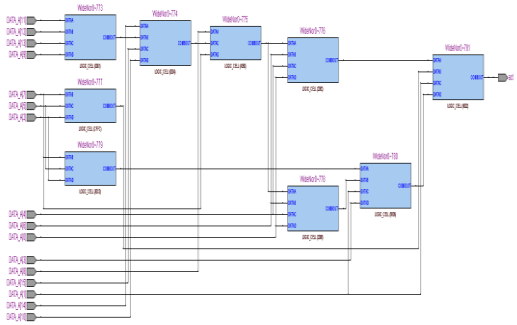

図８．ファイアウォールユニット.

表３．許可するポート番号

Function	Port Number	Binary
NOP	0	0000000000000000
SMTP	25	0000000000011001
DNS	53	0000000000110101
HTTP	80	0000000001010000
POP3	110	0000000001101110
HTTPS	443	0000000110111011

図８のゲートレベルシミュレーションの結果を図９に示す．通常の動作方法では，Winny 検知ユニットよりも低速な 50MHz で動作する．50MHz 動作によって，(1)式より，ギガビットイーサネットに対応させることが可能である．しかし，ギガビットイーサネットと PCI バスと接続の両面を考慮すると, 66MHz 以上で動作することが不可欠である．

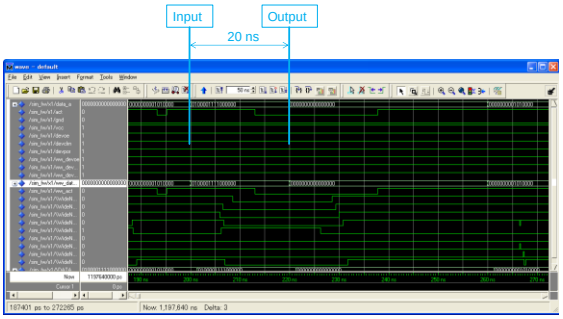

図９．図８の通常動作　(50MHz).

一般に，動作クロック周波数を上げるには，パイプライン手法がある．しかしパイプライン手法は，レジスタを使用するため，消費電力を増大させる原因である[8]. さらに，ファイアウォールユニットは常に動作させることが必要なため，パイプラインレジスタのクロックを制御することも不可能である．

ウェーブパイプライン化動作にて，図８のファイアウォールユニットを動作させると，パイプラインレジスタを使用せずに，高速に動作させることが可能である．また，レジスタを使用していないため，パケットの通過が無い場合の電力消費は微小である．図１０に 100MHz で動作する図８のウェーブパイプライン化動作のゲートレベルシミュレーションの結果を示す.

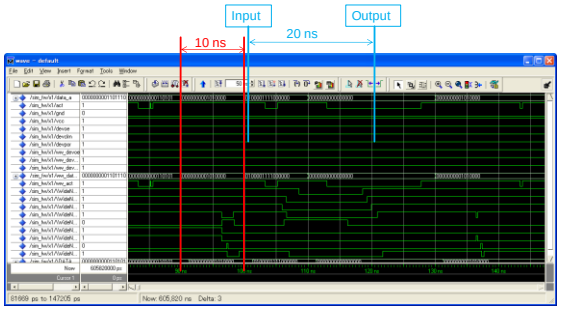

図１０．図８のウェーブパイプライン動作 (100MHz).

クライアント PC にける NIC は，ストリーミング等のアプリケーションを除いて，パケットの送受信を行う時間よりもアイドリング時間のほうが長い．ファイアウォールユニットの消費電力は，QuartusII で解析した結果，120mW であり．Winny 検知ユニットの消費電力は，214mW である．このため，ファイアウォールユニット側で Winny 検知ユニットの動作に必要なクロック信号の制御を行うことで，常に Winny 検知ユニットを動作させるよりも消費電力の削減が可能になる．

6. おわりに

Winny を検知する手法として，暗号化パケットペイロードをエンコードしWinny特有の特徴を解析するシグネチャマッチングすること有効であることは知られている．しかし，ネットワーク機器における実装はキャンパスネットワーク特有の問題及び性能上の問題がある．パソコン自体へのソフトウエアでの実装は，そのソフトウエアによる CPU リソースの消費やアプリケーションの干渉リスクが高まる問題がある．これらの問題を解消するために，Winny 検知ユニットを FPGA に実装し，FPGA をロジックアナライザで実際の動作を測定することで性能評価を行った．

評価結果より，ギガビットイーサネットに対応し，性能の問題を解決できることを明らかにした．消費電力については，ウェーブパイプライン動作ファイアウォールユニットと組み合わせることで削減できることを提案した．

今後の研究では，ウェーブパイプライン動作ファイアウォールユニットを組み合わせたWinny検知ユニットの消費電力の評価およびネットワークに組み込み検知率の評価をおこなう．

謝辞

本研究の一部は文部科学省科学研究費補助金（若手研究(B), 19700050）による実施である．

参考文献

[1] 金子勇, “Winny の技術, “ アスキー, 2005.

[2] T. Karagiannis, A. Broido, N. Brownlee, K.C. Claffy, M. Faloutsos, “Is P2P dying or just hiding?,” Proc. of IEEE Communications Society Globecom 2004, pp.1532-1538, 2004.

[2] 大坐畠智, 川島幸之助, “クライアント／サーバ関係に着目したピュア P2P アプリケーショントラヒック特定方式と評価,” 情報処理学会論文誌, Vol. 49, No. 2, pp.988-998, 2008.

[3] “Winny 個人情報流出のまとめ,” http://www.geocities.jp/winny_crisis/, 2008.

[4] 右田雅裕，杉谷賢一，入口紀男，喜多敏博，中野裕司，松葉龍一，武藏泰雄，辻一隆，島本勝，木田健，平英雄, 太田泰史, 宇佐川毅, 秋山秀典, “全学無線 LAN システムによるユビキタス環境の構築,” 学術情報処理研究, No.8, pp. 17-24, 2004.

[5] 佐藤和洋, “ノート PC 活用教育情報環境の仕様策定とその活用事例報告,” 社会情報, Vol. 13, No. 1, pp. 29-64, 2003.

[6] 斉藤 栄太郎, “Winny の通信解読に挑戦！” http://itpro.nikkeibp.co.jp/article/COLUMN/20060511/237617/, 2006.

[7] Tomoaki Sato, Syuya Imaruoka, and Masa-aki Fukase, “Reconfigurable Firewall Unit by Wave-Pipelined Operations,” Proc. of IEEE ISPACS 2008, 2008 (Submitted).

[8] M. Fukase, T. Sato, R. Egawa, and T. Nakamura, “Breakthrough of Superscalar Processors by Multifunctional Wave-Pipelines,” Proc. of 9th NASA Symposium on VLSI Design, pp. 6.3.1-6.3.17, Nov. 2000.