

ICMP パケットの遮断による IPv6 通信における問題への 対策

近江 敬太^{1,a)} 吉浦 紀晃^{1,b)}

概要: IPv6 では ICMP パケットの遮断が原因で起こるフォールバック問題と Path MTU 問題がある。ICMP パケットが端末に届かない状況下でフォールバック問題や Path MTU 問題が発生した場合、通信に遅延が発生する。本論文では、フォールバック問題か Path MTU 問題が発生した場合、問題が生じている端末へ正規の ICMP パケットと同等な ICMP パケットを送信し、通信の遅延を解消させるシステムを開発した。開発したシステムの有効性を確かめるため実験を行った。実験ではフォールバック問題で起こる通信の遅延は解消できた。

キーワード: IPv6, フォールバック問題, Path MTU 問題, ICMP, デュアルスタック

Resolving Problems caused by denying ICMP packets in IPv6.

OMI KEITA^{1,a)} YOSHIURA NORIAKI^{1,b)}

Abstract: In IPv6, denying ICMP packets causes two problems; one is a problem of fallback in IPv4/IPv6 Dual-Stack environment and the other is that of Path MTU Discovery. Each of the problems delays communication. This paper creates a system that shortens this communication delay. The overview of the system behavior is as follows; the system runs on the gateway of a network and checks the IPv6 traffic of the nodes in the network. The system checks IPv6 communication between the nodes in the network and outside of the network. If the system notices failure of the IPv6 communication, the system sends ICMP packets to the node that is a node of IPv6 communication to prompt fallback of IPv6/IPv4 or adjustment of packet length for path MTU problem. This paper evaluates the performance of the system by experiment, which shows that the system can shorten communication delay that is caused by the fallback problem.

Keywords: IPv6, fallback, Path MTU Discovery, ICMP, dual stack

1. はじめに

インターネットにおいて Internet Protocol Version 4 (以下, IPv4) アドレスが枯渇し, IPv4 から Internet Protocol Version 6 (以下, IPv6) への移行が本格的に行われている。IPv6 は IPv4 の代わりとなるプロトコルとして作られた。しかし, 技術的な問題やコストの問題が原因で IPv4 から IPv6 へ即座に移行することができない。現在のネットワー

クでは IPv4 と IPv6 の両方を使いながら徐々に IPv6 への移行を進めている状態である。IPv6 では Internet Control Message Protocol (以下, ICMP) パケットを利用して通信を行うことがある。ICMP とは IP 通信の機能を補完するためのプロトコルであり, エラーメッセージや制御メッセージを転送する。しかし, ネットワークにおいて ICMP パケットはセキュリティを考慮して遮断されている場合がある。通信に障害が発生した場合, 通信を行っている端末は ICMP パケットを受信することにより障害の原因や次に行うべき処理を知ることができるが, ICMP パケットを受け取れない状況下では障害の原因や次に行うべき処理を知ることができないため通信に遅延が発生してしまう。IPv6

¹ 埼玉大学大学院理工学研究科数理電子情報部門情報領域
Department of Information and Computer Science, Saitama University

a) omi@fmx.ics.saitama-u.ac.jp

b) yoshiura@fmx.ics.saitama-u.ac.jp

では ICMP パケットが遮断されていることが原因で起こる問題としてフォールバック問題と Path MTU 問題がある。

本論文ではフォールバック問題や Path MTU 問題で起こる通信の遅延を解消するシステムを開発する。ICMP パケットが届かないことによりフォールバック問題や Path MTU 問題が発生した場合、本来届くはずの ICMP パケットと同等の ICMP パケットを開発するシステムが作成し、フォールバック問題と Path MTU 問題で起こる通信の遅延を解消させる。

関連研究として [1] があり、IPv6/IPv4 フォールバックに関する問題提起とその解決方法が述べられている。また、フォールバック問題と ICMP パケットの関係も述べられている。しかし、[1] では、フォールバック問題に対する ICMP パケットの利用に関しては消極的であった。OS によって ICMP パケットを受け取ってもフォールバックが起こらない場合があるからである。[1] では OS に問題があると述べられている。そこで、本論文では ICMP パケットを利用したフォールバック問題の解決をはかる。本論文では実際にシステムを開発し、フォールバック問題と Path MTU 問題が解決できるかどうかを試し、ICMP パケットを利用したシステムの有効性を示す。

2. ICMP パケットの遮断によって起こる IPv6 通信における問題

IPv6 通信において ICMP パケットの遮断が原因で起こる問題に、フォールバック問題と Path MTU 問題がある。

2.1 フォールバック問題

フォールバック問題は IPv4 と IPv6 の両方を扱えるようなデュアルスタック環境で発生する。インターネットにおいて他のノードと通信を行う場合、通信相手の IP アドレスを取得するために DNS(Domain Name System) で問い合わせ通信相手の IP アドレスを取得する。デュアルスタック環境下では通信相手の IP アドレスとして IPv4 アドレスと IPv6 アドレスの両方を得る場合がある。

図 1 のように IPv6 での通信が失敗した場合、IPv4 での通信に切り替える動作、逆に、IPv4 での通信に失敗し、IPv6 での通信に切り替える動作をフォールバックという。端末は経路途中におけるルータ等から送信される ICMP パケットを受け取ることでフォールバックを行うことができる。しかし、経路途中で ICMP パケットが遮断されている等により ICMP パケットが端末に届かない状況では、端末はフォールバックを行うためのきっかけを失う。フォールバックを行うきっかけを失った端末は行うべき処理がわからないため、通信に遅延が生じる。

2.2 Path MTU 問題

Maximum Transmission Unit (以下、MTU) とは隣の

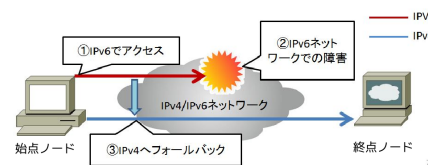


図 1 フォールバック

Fig. 1 Fallback.

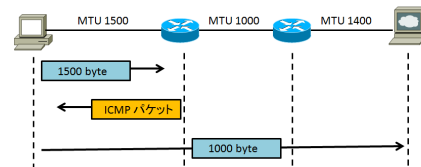


図 2 Path MTU Discovery

Fig. 2 Path MTU Discovery.

ネットワークに転送できるパケットの最大サイズである [2]。また、Path MTU とは通信を行う際の始点ノードから終点ノード間での最小の MTU である。IPv4 では経路途中でのパケットの分割が可能であるが、IPv6 では経路途中でのパケットの分割ができないため始点ノードは予め終点ノードへの Path MTU を知らなければならない。Path MTU を知るための機能として Path MTU Discovery がある。

Path MTU Discovery とは ICMP パケットのエラーメッセージであるパケット過大を利用した機能である。図 2 のように、はじめに始点ノードの繋がっている MTU のサイズのパケットを送信し、パケットのサイズが経路上の MTU の値を超えていた場合には始点ノードに ICMP パケットが返ってくる。返ってきた ICMP パケットには次に送るべき MTU のサイズの情報があり、その情報をもとにして次に送るパケットのサイズを調整する。

ICMP パケットが始点ノードに届かない場合、Path MTU Discovery が動作しないため Path MTU の取得ができず通信の遅延が発生する。

3. システム概要

システムはパケットをキャプチャし、フォールバック問題や Path MTU 問題を解決するための情報を取得する。このシステムはネットワークのゲートウェイで動作させる。システムは端末上で動作させることも可能であるが、ゲートウェイで動作させることにより複数の端末と情報を共有することができる。ゲートウェイでシステムを動作させることにより複数の端末から送信されるパケットを取得することで多くの情報を得ることができる。また、ゲートウェイでシステムを動作させることにより各端末にシステムを導入する必要がなくなる。システムは IPv6 から IPv4 へのフォールバック時のみに動作するものを作成した。Path MTU 問題においては IPv6 で起こる場合にのみ動作するものを作成した。また、TCP 通信で動作するものを作成

した．

システムは主に以下の動作を行う．

- パケットキャプチャ
- 通信状態の分析
- ICMP パケットの作成と送信
- 処理方法の記録

3.1 システムの流れ

システムは図 3 のように動作する．システムはパケットをキャプチャする．キャプチャしたパケットから情報を読み取る．システムの動作はパケットから得られる情報により分岐する．動作の分岐に必要な情報はシステムに記録する．システムは図 4 のように始点ノードと終点ノードとの通信状態を分析し、通信が成功しているかどうかを判断する．通信が失敗していると判断した場合、システムは始点ノードに ICMP パケットを送信する．その後、システムは通信が成功するかどうかを確認するために再び通信状態を分析する．システムは以上の動作から、分析していた通信に対してどの処理を行うべきかを判断し、処理方法を記録する．システムは通信の遅延を小さくするため、次回以降の通信で記録された処理方法を参照し、即座に適切な処理を行う．

3.2 パケットのキャプチャ

システムは常にパケットをキャプチャする．システムはキャプチャしたパケットから情報を読み取る．システムはパケットから読み取った情報を表 1 のように記録する．システムは IP アドレス情報とパケットサイズをパケットから読み取り記録する．記録する IP アドレス情報は始点ノードから送信されたパケットの宛先 IP アドレスである．パケットサイズの情報は通信の最中で送受信されたパケットの最大サイズを記録する．記録した情報は図 3 にあるように、システムの処理の分岐で使う．また、IP アドレスとパケットサイズの情報は表 1 のように対応付けて記録する．

3.3 処理フラグ

システムはアドレスリストの IP アドレスとキャプチャした IP アドレスが一致した場合に、処理フラグにもとづき動作する．表 1 の処理フラグはシステムに記録された IP アドレスへの通信に対して行うべき処理を記録したもので

表 1 記録する情報の例

Table 1 Example of system of memory.

IP アドレス	最大パケットサイズ	処理フラグ
ABCD	1280	Path MTU 問題
EFGH	78	フォールバック
IJKL	400	再分析
MNOP	1440	通過

ある．処理フラグは以下の 4 種類である．

- 通過
- 再分析
- フォールバック
- Path MTU 問題

処理フラグの「通過」はパケットを通過させる．「再分析」は通信を再び分析する．「フォールバック」はフォールバックで使用される ICMP パケットを送信する．「Path MTU 問題」は Path MTU 問題で使用される ICMP パケットを送信する．

3.4 通信状態の分析

システムは通信状態を分析し、通信が成功しているかどうかを判断する．

システムは通信が成功しているかどうかを判断するために外部のネットワークから送信されるパケットを一定時間キャプチャする．一定時間内でキャプチャしたパケットの中に通信相手から送信されるパケットがある場合、システムは通信が成功していると判断する．逆に、一定時間が経過しても通信相手から送信されるパケットがない場合、システムはフォールバック問題か Path MTU 問題が原因で通信が失敗していると判断する．

システムはフォールバック問題と Path MTU 問題の 2 つの問題に対応する．システムの各問題に対する処理方法は異なる．従って、システムは通信が失敗したと判断した場合、フォールバック問題か Path MTU 問題のどちらが起きているのかを判断する必要がある．TCP の通信ではコネクションを確立させるためにスリーウェイハンドシェイクを行う．システムはスリーウェイハンドシェイクの段階でフォールバック問題と Path MTU 問題の区別をする．

3.4.1 フォールバック問題の特定方法

フォールバック問題が発生する場合、通信相手との IPv6 通信に障害があり、通信ができない状態である．スリーウェイハンドシェイクでは通信の始点となる端末が始点が SYN パケットを送信する．IPv6 通信に障害がある場合、通信の始点となる端末が送信した SYN パケットが通信相手に届かないため、SYN+ACK パケットが通信の始点となる端末に返ってこない状態になる．システムは通信の始点となる端末が SYN パケットを送信したにも関わらず、通信相手からの SYN+ACK パケットが送信されてこない場

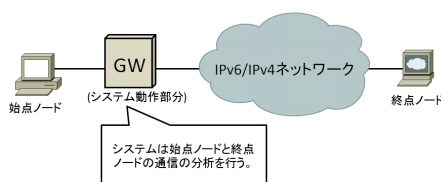


図 4 通信状態の分析

Fig. 4 Analyzing Communication.

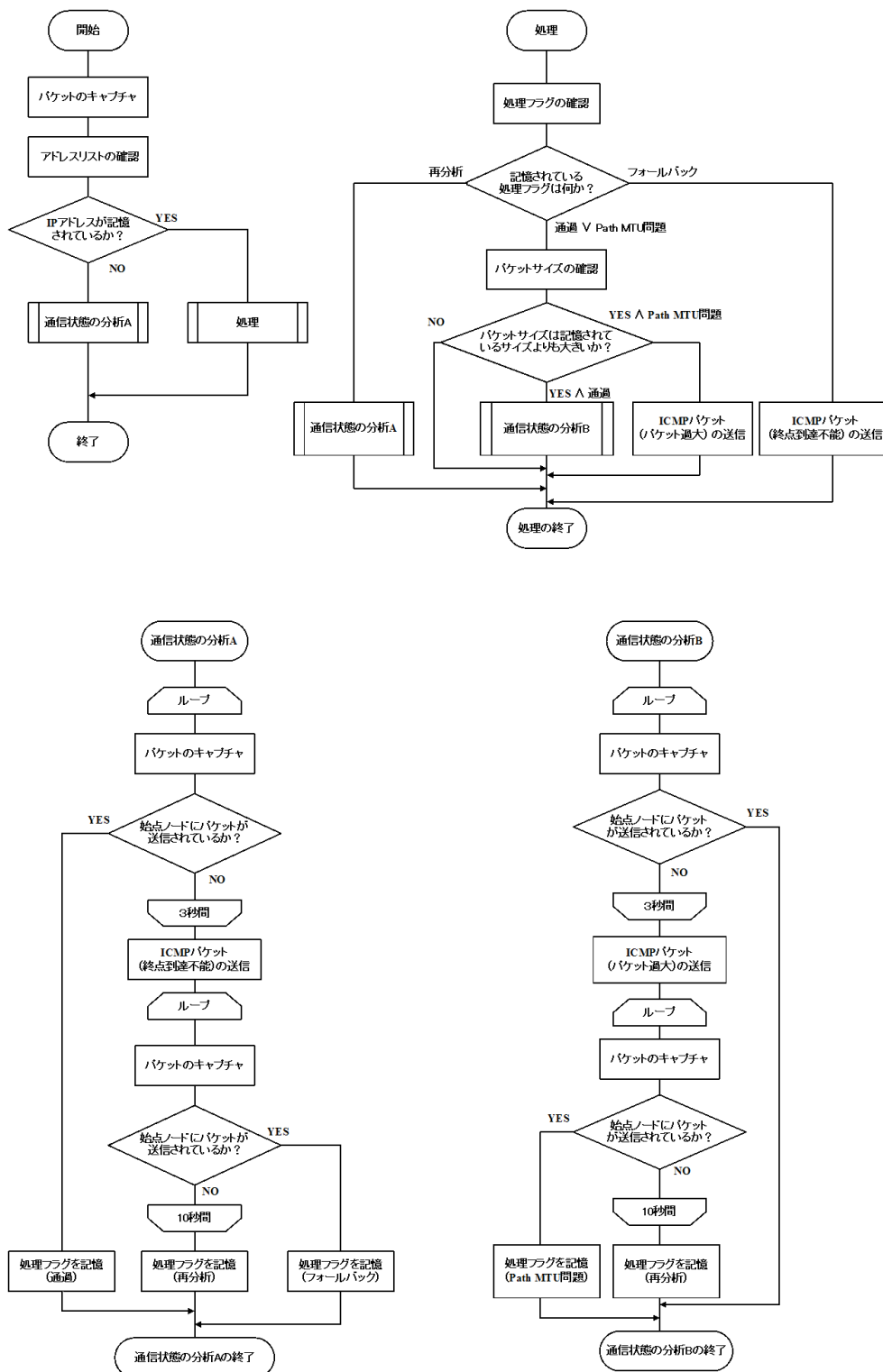


図 3 システムの流れ
 Fig. 3 System flow chart.

合にフォールバック問題が発生していると判断する。

3.4.2 Path MTU 問題の特定方法

Path MTU 問題は通信の最中で大きなサイズのパケットを送信する場合に発生する。スリーウェイハンドシェイクでやりとりされるパケットのサイズは小さいものである。従って、スリーウェイハンドシェイクの段階では Path

MTU 問題は発生しない。Path MTU 問題はフォールバック問題とは異なりコネクションが確立した状態で発生する。システムはコネクションが確立した後の通信において、大きなサイズのパケットが通信の始点となる端末から送信された場合、通信状態の分析を行う。システムは通信状態の分析を行い、通信が失敗したと判断した場合、Path MTU

問題が発生している」と判断する。

システムは問題が発生し通信が失敗していると判断した場合、内部ネットワークにおける通信の始点となる端末に、問題に対応する ICMP パケットを作成し送信する。

3.5 ICMP パケットの作成と送信

ICMP には IPv4 用の ICMPv4 と IPv6 用の ICMPv6 がある。本論文では ICMPv6 のみを扱う。

ICMP パケットは図 5 のような構造している。

図 5 における Type フィールドは ICMP メッセージのタイプであり、Code フィールドはメッセージに対する付加情報を示すものである。また、Message Body には Type と Code によって入る情報が異なる。

表 2 は ICMPv6 におけるメッセージの一部である。

システムは通信経路上で遮断された ICMP パケットと同等の ICMP パケットを作成し送信する。ICMP パケットの作成は [3], [4] を参考にした。

フォールバックを始点ノードに行わせるために送信する ICMP パケットは終点到達不能である。終点到達不能の ICMP パケットを作成するためにシステムに始点ノードから送信されたパケットから IP ヘッダと TCP ヘッダを取得させ、取得した IP ヘッダと TCP ヘッダを ICMP パケットの Message Body に設定した。

Path MTU 問題に対応する ICMP パケットはパケット過大である。本論文で作成したシステムで作成するパケッ

ト過大の ICMP パケットは、IPv6 において最低限保証されている MTU の値である 1280 バイトを修正させるパケットサイズとして設定した。

3.6 フォールバックにおける通信成功の判断方法

システムは通信状態の分析を行い、通信が成功したかどうかを判断する。3.4 節で説明したように、システムは通信相手から送信されるパケットがある場合に通信が成功したと判断する。システムはパケットの送信元 IP アドレスを見て通信相手から送信されたパケットであると判断する。Path MTU 問題では、問題の解決前後でやりとりされるパケットは IPv6 で統一されているため、キャプチャしたパケットから得られた IP アドレス情報のみで通信の成功の判断できる。しかし、フォールバックにおいては、通信が IPv6 通信から IPv4 通信に切り替わるため、通信が成功したかどうかの判断のために新たに IPv4 アドレスの情報が必要となる。また、システムはフォールバックが成功したと判断するために通信相手の端末に割り振られている IPv4 アドレスと IPv6 アドレスを対応付ける必要がある。作成したシステムでは IPv4 アドレスの取得と、IPv4 アドレスと IPv6 アドレスの対応付けに逆引きと正引きを利用する。IPv6 アドレスから逆引きを行い、端末のホスト名を取得し、取得したホスト名から正引きで IPv4 アドレスを取得し、端末に割り振られている IPv4 アドレスと IPv6 アドレスの対応付けを行う。

4. 実験

4.1 実験環境

本論文で作成したシステムは本来ゲートウェイで動作させることを目的としている。しかし、今回行った実験ではシステムを端末で動作させて行った。

現在のネットワークにおいてフォールバック問題や Path MTU 問題が発生する IPv6 の通信が見つからないため、問題が発生するような環境を作成して実験を行った。作成した実験環境下において、本論文で作成したシステムを動作させた場合と、作成したシステムを動作させない場合で、IPv6 に対応している Web サイトにアクセスを試み、通信の状態を比較し、システムの有効性を確認する。アクセスを試みた IPv6 に対応している Web サイトの数は 60 サイトである。

また、実験では表 3 の機材を使用した。

4.1.1 フォールバック問題が発生する環境作成

ファイアウォールで IPv6 パケットを遮断するようにした。内部ネットワークから外部のネットワークに IPv6 の通信を試みた際、フォールバック問題が発生するようにした。

4.1.2 Path MTU 問題が発生する環境作成

ファイアウォールで外部からの ICMP パケットを遮断

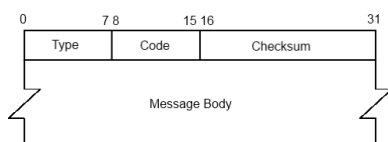


図 5 ICMP パケットの構造

Fig. 5 Structure of ICMP packet.

表 2 ICMPv6 メッセージの一部

Table 2 ICMPv6 Message.

Type	Code	メッセージ
1		終点到達不能:
	0	終点への経路がない
	1	管理上禁止
	2	非近隣ノード
	3	アドレス到達不能
2	4	ポート到達不能
	0	パケット過大
3		時間経過:
	0	ポップ限界到達
	1	フラグメント再構成時間経過

した．また，実験でアクセスする Web サイトは始点ノードからの終点ノードへの Path MTU が始点ノードの MTU より小さくなる箇所を選び通信を試みることで作成した．

4.2 実験結果

フォールバックに関する実験では表 4 のような結果になった．開発したシステムではフォールバックが成功したことを判断できない場合があった．開発したシステムでは IPv6 アドレスと IPv4 アドレスの対応付けに逆引きと正引きを利用した．しかし，現在のインターネットでは IPv6 アドレスの逆引き登録を行っている箇所が少なく，作成したシステムの動作が機能しない場合が多くあった．今回の実験でアクセスを試みた Web サイトのうち 36 サイトで逆引きを行うことができなかった．

Path MTU 問題に対応するシステムは作成したが，Path MTU 問題は発生する IPv6 通信を発見することができなかった．従って，Path MTU 問題に関する実験の結果をとることができなかった．

5. 考察

IPv6 の通信において，ICMP パケットが経路途中で遮断され，通信の始点となる端末に ICMP パケットが届かないことが原因でフォールバック問題が発生した場合，システムが正規の ICMP パケットと同等の ICMP パケットを端末に送信することにより通信の遅延を解消することができた．

フォールバック問題に対する実験結果で通信の成功までの時間が約 4 秒であるが，これは開発したシステムが通常の通信が成功したかどうかを 3 秒待ち，その後にフォールバック問題に対応する終点到達不能の ICMP を送信するからである．本論文では通信の成功を判断するための待ち時間の最適値を検討していない．従って，今後は待ち時間の調整を行う必要がある．

本論文で開発したシステムではフォールバックが成功したかを判断する機能が不完全であることがわかった．システムが ICMP パケットを端末に送信することによって，フォールバックが成功したかを確認するためには，通信相

手の IPv4 アドレスと IPv6 アドレスの両方をシステムが知らなければならない．本論文で開発したシステムでは IPv6 アドレスから逆引きを行いホスト名を取得し，取得したホスト名から正引きを行い IPv4 のアドレスを取得する方法をとった．しかし，IPv6 アドレスの逆引きの登録を行っている箇所が少なく，IPv6 アドレスからホスト名の逆引きができない箇所が多いため，IPv4 アドレスと IPv6 アドレスの対応付けの方法を再度考える必要がある．

Path MTU 問題が起こる IPv6 の通信を発見することができなかった．従って，作成したシステムの Path MTU 問題に対する有効性を確認することができなかった．Path MTU 問題に対する実験方法について再度考える必要がある．

6. おわりに

本研究では ICMP パケットの遮断により始点ノードに ICMP パケットが届かない状況で起こるフォールバック問題と Path MTU 問題を解決するためのシステムの開発を行った．開発したシステムによってフォールバック問題で起こる通信の遅延を解消することができた．

本研究で開発したシステムは，フォールバックが成功したかどうかの判断には IPv6 アドレスと IPv4 アドレスの対応付けを必要とする．アドレスの対応付け方法として，IPv6 アドレスからホスト名の逆引きを行い，得られたホスト名から IPv4 アドレスを正引きを行い IPv6 と IPv4 アドレスの対応付けを行った．しかし，IPv6 アドレスの逆引き登録を行っている箇所は少なく IPv4 アドレスと IPv6 アドレスの対応付けが不完全であった．そのため，フォールバック問題で起こる通信の遅延は解消されているが，システムがフォールバックが成功したかを判断することができず，2 回目以降の通信において行うべき処理をシステムに記録させることができないことがあった．

Path MTU 問題が発生する IPv6 の通信を発見することができなかったため，開発したシステムの有効性を確認することができなかった．

参考文献

- [1] 藤崎 智宏, 新延 史郎, 松本 存史, "IPv6/IPv4 デュアルネットワークにおけるフォールバック問題に関する考察", 情報処理学会, 情報処理学会研究報告 分散システム/インターネット運用技術, 2007 (93), pp.37-42
- [2] RFC 791 INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION: 入手先 <http://tools.ietf.org/html/rfc791>
- [3] RFC 792 INTERNET CONTROL MESSAGE PROTOCOL: 入手先 <http://tools.ietf.org/html/rfc792>
- [4] RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification: 入手先 <http://tools.ietf.org/html/rfc4443>

表 3 実験機材

Table 3 Experimental equipment.

OS	Vine Linux2.6.35-21vl6
CPU	Intel(R) Core(TM)2 Duo 1.06GHz
メモリ	2GB

表 4 フォールバック問題における実験結果

Table 4 Experimental results of fallback.

	システムを動作してない場合	システム動作時
平均値	205.29 秒	3.96 秒