2007－DSM－47 (7)
2007／9／21

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

藤崎 智宏† 新延 史郎† 松本 存史†

†NTT 情報流通プラットフォーム研究所 〒180-8585 東京都武蔵野市緑町 3-9-11

E-mail: †fujisaki.tomohiro@lab.ntt.co.jp, nin@syce.net, arifumi@nttv6.net

あらまし インターネットの利用が拡大し，利用者の増加，利用目的の多様化が顕著である．このような拡大に対応するために，現在のインターネットプロトコル（IPv4）の後継としてバージョン 6（IPv6）が標準化され，実利用が進んでいる．現状では，IPv6 は IPv4 と同一環境上（デュアルスタック環境）で利用されることが多い．インターネットではネットワークノードの名前（FQDN）は，IPv4 と IPv6 で同一であることなどからデュアルスタック環境では，通信手段の選択に関わる問題が発生する．

本稿では，デュアルスタック環境において発生する，IPv6/IPv4 通信フォールバック問題について現状を分析し，解決方法を提案する．

Communication fallback problem in the IPv6/IPv4 dual stack environment

Tomohiro FUJISAKI† Shirou NIINOBE‡ and Arifumi MATSUMOTO‡

†NTT Information Sharing Platform Laboratories 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan

E-mail: †fujisaki.tomohiro@lab.ntt.co.jp, nin@syce.net, arifumi@nttv6.net

Abstract Today, the Internet is widely used in varied ways, and lots of devices are connected. To cover these advanced usage, a new version of the Internet protocol, IPv6 was standardized as a successor protocol of IPv4 and come into use. Currently, in many cases, IPv6 is used with IPv4 at the same time in a dual-stack environment. In that environment, if a node tries to communicate with another node which has both IPv4 and IPv6 address, the node tries to use IPv6 first. If the IPv6 communication fails, the node retries its communication with IPv4. This communication switch takes a long time.

In this paper, we examine the communication switch problem in detail, and propose solutions to prevent that problem.

1 はじめに

近年，インターネットの利用が拡大し，利用者の増加，利用目的の多様化が顕著である．このような拡大に対応するために，現在のインターネットプロトコル（IPv4）の後継としてバージョン 6（IPv6）が標準化され，実利用が進んでいる．

現状では IPv4 が広く利用されており，IPv6 は IPv4 と同一環境上（デュアルスタック環境）で利用されることが多い．インターネットではネットワークノードの名前（FQDN）は，IPv4 と IPv6 で同一であることなどからデュアルスタック環境では，通信手段の選択に関わる問題が発生する．

本稿では，デュアルスタック環境において発生する，IPv6/IPv4 通信フォールバック問題について現状を分析し，解決方法を提案する．第 3 章に

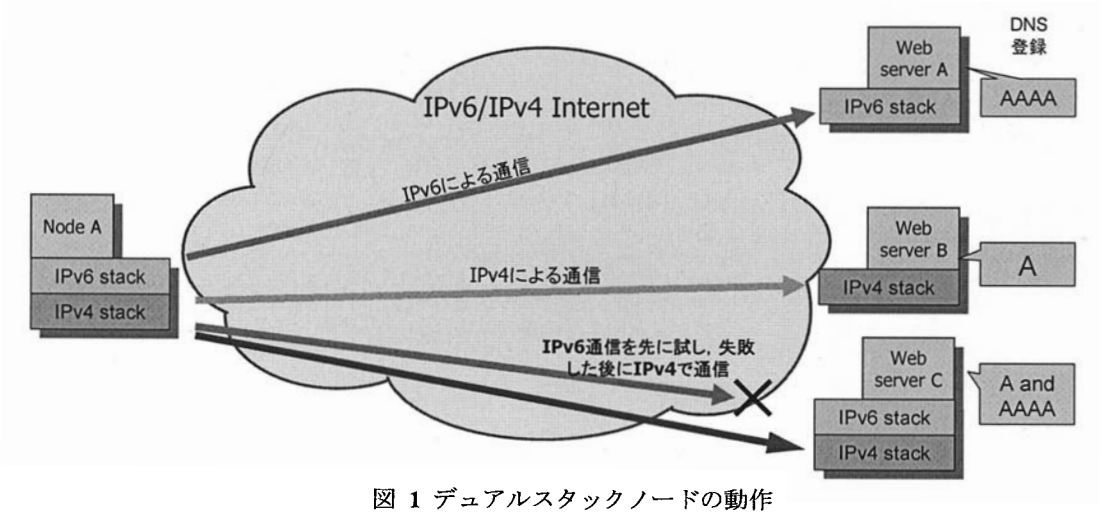

図 1 デュアルスタックノードの動作

て，フォールバック問題を詳説し，第 3 章にて関連仕様，関連研究について述べる．第 4 章にて，既存システムのフォールバック動作検証結果を詳説し，第 5 章にて解決策の提案，及び既存システムでの実証結果を述べ，第 6 章にてまとめを述べる．

2 IPv4 と IPv6 の共存

2.1 IPv6 の標準化

現在広く利用されているインターネットのベースとなっているインタネットプロトコル(IPv4)は，インターネットの拡大過程で発生したいくつかの問題に対し，その都度対処，修正を行い，現在に至っており，基本的な部分は標準化当初とほとんど変更なく利用されている．しかしながら，近年の爆発的なインターネットの規模の拡大により，32bit のアドレス空間の不足，インターネットの複雑化を原因とする経路情報の肥大化といった，インターネットプロトコルの根幹に関わる問題が顕在化してきている．

また，インターネットの利用が拡大し，インターネットの利用者・利用目的が多様化することにより，インターネット接続時の設定の簡素化，インターネット通信におけるセキュリティの確保，動画・音声などのリアルタイム通信の実現といった新たな要求が発生している．

このような状況の中で，インターネット関連技術の標準化団体である IETF(Internet Engineering Task Force) にて，IPv4 の後継プロトコルとして，インターネットプロトコル IPv6(Internet Protocol version 6)[1]が標準化された．

2.2 IPv6 と IPv4 の同時利用

IPv6 はプロトコル的には IPv4 と互換性はなく，IPv6 を実装したノードと IPv4 を実装したノードは直接通信できない．このため，現状多くのノードは，IPv6 と IPv4 の両機能を持つ，デュアルスタックノードとして実装されている．通信を開始する際，ノードは，通信相手が IPv6 ノードか IPv4 ノードかによって，利用するプロトコルを選択して通信を実施する．

インターネットにおいては，ネットワーク中のサーバなどのノードは，FQDN（Fully Qualified Domain Name）という階層的な名前にて識別される．IPv6 と IPv4 では，この FQDN は同一の名前空間を利用しており，一つの名前に対して，IPv6 アドレスと IPv4 アドレスの両方，もしくはどちらかが対応づけられている．ノードは，通信を開始する際，ドメインネームシステム（DNS）を利用し通信相手の FQDN に対応づけられている IP アドレスを取得する．通信相手のアドレスとして，IPv6 アドレス（AAAA レコード）と IPv4 アドレス（A レコード）のどちらか，または両方が得られることになる．通信相手のアドレスとして，IPv4, IPv6 の両方のアドレスが得られた場合には，ノードの初期動作として，IPv6 通信を先に試すことが RFC3484[2] にて規定されている．

3 IPv6/IPv4 フォールバックとその問題

3.1 IPv6/IPv4 フォールバックとは

図 1 に，デュアルスタックノードが IPv6 ノード，IPv4 ノード，および IPv6/IPv4 デュアルスタックノードと

通信する様子を示す．上記のように，通信相手がデュアルスタックノードの場合，ノードはまずIPv6を使った通信を実施しようとする．何らかの原因で，このIPv6通信が失敗したときに，ノードはIPv4での通信を試す．この，IPv6通信からIPv4通信への切り替わりを「IPv6からIPv4へのフォールバック」と定義する．

IPv6から，IPv4へのフォールバックは，プロトコル非依存プログラミング[3]で推奨されているプログラミングスタイルをとったアプリケーションの標準的な動作である．

3.2 IPv4/IPv6フォールバックの発生

IPv6/IPv4フォールバックは，IPv6接続性が安定していない場合や，障害などによりIPv6通信ができない場合に発生する．以下に，その例を挙げる．

- 管理されていないIPv6/IPv4共存・移行メカニズム（6to4[4]などの自動トンネル）など，品質の悪いIPv6接続性を利用している場合
- サーバが，IPv6アドレス（AAAAレコード）をDNSに登録しているが，IPv6での接続性を持っていない場合
- IPv6グローバルインターネットへの接続性がないネットワークを用いている場合（VPNや，ULA[5]を利用した社内ネットワーク，閉域ネットワークなど）

フォールバックが発生した場合，IPv6通信からIPv4通信への切り替わりに時間がかかることがある．たとえば，Webアクセスをしているユーザにとっては，Webページが表示されるまでに20秒程度待たされる場合があり，ネットワークのユーザビリティに大きく影響する．

3.3 障害情報の通知

ネットワークに障害があった場合など，IPv6通信に問題があるには，障害情報がネットワークからノードに通知されることが一般的である．図2に，IPv6通信経路がない場合に，通信の始点ノードに障害が通知される例を示す．

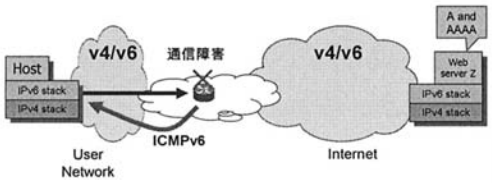

図 2 ICMPv6による障害通知

通信障害が発生した場合，ネットワークからノードに対して，障害の理由を示すエラーがICMPv6により通知される．表1に，IPv6で定義されている主なICMPv6メッセージを示す．

型(Type)	名称	定義文書
1	終点到達不能	RFC2463[6]
2	パケット過大	RFC2463
3	有効期間超過	RFC2463
4	パラメータ異常	RFC2463
128	エコー要求	RFC2463
129	エコー応答	RFC2463
139	ノード情報要求	RFC4620[7]
140	ノード情報応答	RFC4620

表 1 ICMPv6メッセージ

ICMPv6メッセージは，「型（Type）」フィールドの値により，区別される．エラー通知用メッセージは，0～127までの値を持ち，情報提供用のメッセージは128～255までの値を持つ．通信障害の際にネットワーク側より通知されるのは，このうち「1」の終点到達不能メッセージで，このメッセージには，障害の原因を示す値（コード（Code）値）が含まれる．表2に，主なICMPv6終点到達不可能メッセージを示す．

コード	名称	定義文書
0	終点までの経路なし	RFC2463
1	終点との通信禁止	RFC2463
2	始点アドレスのスコープ超	RFC4443[8]
3	アドレス不達	RFC2463
4	ポート不達	RFC2463
5	出入ポリシ始点アドレス誤	RFC4443
6	終点向経路不許可	RFC4443

表 2 終点到達不可能メッセージの種類

IPv6ノードは，ネットワークから特定のエラーメッセージを受信した場合，IPv6通信からIPv4通信へのフォールバック動作を実施することが期待される．

また，昨今，セキュリティ確保の目的から，外部からのICMPを遮断することも多いが，デュアルスタックネットワークでは，通信障害を通知するICMPは，ノードまで到達するように設定すべきである．

3.4 障害通知メッセージに対する動作

インターネットノードがTCP通信を実施している際に，ネットワークからICMPエラーを受け取った場合の動作は，RFC1122[9]に規定されている．このRFCでは，ICMPメッセージをネットワークの一時的通信障害（経路異常など）であり，回復の可能性のある「ソ

フトエラー」と，恒久的な通信障害である「ハードエラー」に分類し，ハードエラーを受信した場合にはTCP通信を切断するが，ソフトエラーを受信した場合はTCP通信を切断してはいけないと定義している．しかしながら，これはIPv4のICMP（以下，ICMPv4）に対する定義であり，現状，ICMPv6に対するTCP通信の動作に関する定義は存在しない．

これに対して，最近のインターネット環境を考慮した上で，旧来のTCPの動作を見直す動きがある．特に，セキュリティ関連を考慮した動きであり，ICMPv6に対する対処としても，[10]のような提案が存在する．この文書では，ICMPv6メッセージをICMPv4メッセージと対応させ，昨今のネットワークの安定性を考慮し，ソフトエラーでもTCP接続を切断すること，切断しない場合でも，接続開始時にソフトエラーを受信した場合には，接続を早期にあきらめることを提案している．

4　ノードのフォールバック動作

4.1　フォールバックにかかる時間

ノードのフォールバック動作を確認するために，実験を実施した．図3に，実験環境を示す．

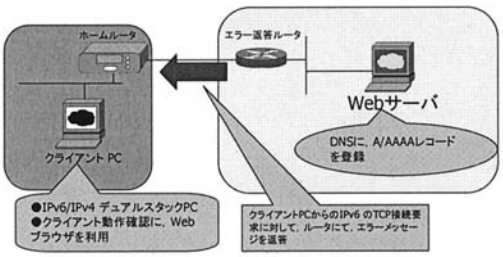

図 3　フォールバック実験環境

クライアントPCは，IPv6/IPv4デュアルスタックネットワークに接続されている．通信相手のWebサーバは，そのIPv6アドレスとIPv4アドレスがDNSサーバに登録されており，クライアントPCがWebサーバに通信をする際には，IPv6による通信が先に実施される．Webサーバとクライアント PCの間にルータを配置し，クライアントPCが開始したIPv6通信に対して，エラーを返答できるように設定する．この環境で，クライアントPCが開始したIPv6 TCP通信について，

- 網からエラーを通知せずに通信を遮断した場合
- コード0～6までのICMPv6終点到達不可能メッセージを返答した場合
- TCPのResetを実施した場合

に関して，それぞれクライアントPCがIPv6通信からIPv4通信に切り替えるのにかかる時間を測定した．測定した結果を表3に示す．それぞれの値は，クライアントPCが最初のIPv6 TCP SYNパケットを送出してから，フォールバックが起こり，最初のIPv4 TCP SYNパケットを送出するまでにかかった時間(秒)である．

4.2　フォールバック時間に関する考察

表からわかるように，Windows Vistaではネットワークから通信障害をICMPv6によって通知された場合でも，IPv6通信からIPv4通信にフォールバックするためにかかる時間は，エラーを通知せず，TCPのタイムアウトによりフォールバックする時間とほぼ同じであり，ICMPv6によるフォールバック動作を実施しないことがわかる（IPv6機能を活かしたWindows XPで

OS	Browser	No Error	Type=1(Destination Unreachable)							TCP reset
			Code=0	Code=1	Code=2	Code=3	Code=4	Code=5	Code=6	
Windows Vista Home Basic	IE	19.99	21.00	20.99	21.00	20.99	20.99	20.99	20.99	1.01
	FireFox	21.00	21.00	21.00	21.00	20.99	20.99	20.99	20.99	1.01
Windows Vista Enterprise	IE	21.06	21.00	20.99	21.00	20.99	21.00	21.01	21.00	1.01
	FireFox	20.99	21.00	20.99	20.99	21.00	21.00	20.99	21.00	1.00
Mac OSX (10.4.8 8L2127)	Safari	74.79	11.80	11.83	17.37	11.68	11.75	74.86	74.89	0.01
	FireFox	74.91	11.61	11.73	11.70	No fallback	11.63	74.79	74.77	0.01
FreeBSD (R6.2-#p1)	FireFox	74.99	12.61	12.61	12.69	No fallback	12.61	74.99	74.99	0.01
Fedora Core 6 (kernel-2.6.20)	FireFox	188.98	0.01	0.01	0.01	0.01	0.0.1	No fallback	No fallback	0.01

表 3　フォールバック時間測定値　（秒）

も同様の動作である)．これに対し，MacOS は，その通信スタックが，FreeBSD 由来のものあり，FreeBSD と同様の動作をしていることがわかる．FreeBSD では，3.4 節で述べたドラフト提案[10]の，TCP 通信開始時に ICMPv6 を受信した場合の処理を実装しており，何もエラーを受信しなかった場合の TCP タイムアウトにかかる時間よりも早いタイミングで，フォールバックが発生している．Linux では，ドラフト提案[10]の，ソフトエラーにおけるフォールバックの実施を既に実装しているため，ネットワークから ICMPv6 エラー返答があった場合には，即座にフォールバックを実施する．なお，MacOS, FreeBSD の 終点到達不可能メッセージコード３は，IPv4 のハードエラーに対応するため，動作を特別扱いしているためフォールバックをしないものと思われる．まだ，コード 5,6 が定義されたのは比較的最近であり，このコードに対する動作が定義されていないため，MacOS, FreeBSD, Linux において動作の違いが発生していると考えられる．

また，現状，ICMPv6 エラー通知に対するオペレーティングシステムごとの動作はまちまちであるが，TCP 通信の場合には TCP Reset を実施することで，フォールバックにかかる時間をなくすことが可能である．

5 フォールバック問題への対応

前述のように，IPv6/IPv4 デュアルスタックネットワークでは，どちらかのプロトコルのネットワークに障害があった場合にフォールバックが発生する．多くのオペレーティングシステムでは，初期状態では IPv6 通信を優先するようになっているため，IPv6 ネットワークの通信品質が悪い場合にフォールバック問題が発生する可能性があり，また，ネットワークから ICMPv6 に障害通知がきた場合でも，フォールバックに時間がかかることになる．この場合，ユーザのネットワークユーザビリティが低下する．

フォールバック問題に対しては，以下のような対処が考えられる．

1. アドレス選択技術（RFC3484）の利用
   VPN などの閉域網とインターネットの併用時など，IPv6 通信を実施する通信先の IPv6 アドレス空間があらかじめわかっている場合には，その空間との通信時のみ，IPv6 を利用し，その他のインターネットアクセスでは IPv4 を利用するような設定をすることができる．また，IPv6 通信よりも IPv4 通信を優先するような設定も可能である．RFC3484 は，多くのオペレーティングシステムで実装されている[11].
2. 経路設定の利用
   1 と同様に，通信を実施する IPv6 アドレス空間が明確な場合，ノードに経路設定を実施することで，特定の場合のみ IPv6 通信を実施するような設定が可能である．ノードに経路を設定するには，RFC4191[12]で定義されているルータ広告の拡張が可能であるが，RFC4191 を実装しているオペレーティングシステムは現状，多くはない．
3. TCP Reset の利用
   IPv6 接続性の品質が悪い通信相手が明確の場合には，そのアドレス空間との IPv6 TCP 通信が発生した際に，TCP Reset を返却することで，IPv4 へのフォールバックを強制することができる．TCP Reset を受け取った際に TCP セッションを切断する動作は TCP の標準動作であり，ほとんどの TCP 実装で意図通り動作すると考えられる．しかしながら TCP 以外のプロトコルには適用できない．

ノードの標準動作として，ネットワークからの ICMP によるエラー通知があった場合に，フォールバックを実施するようにすべきであると考えられる．現在，IETF のトランスポートエリアで，トランスポートプロトコルの ICMP への対応を標準化する議論が実施されている．

6 まとめ

本稿では，IPv6/IPv4 デュアルスタックネットワークで発生する，IPv6/IPv4 フォールバックに関する問題提起とその解決方法について述べた．IPv6 がインターネット上で広く使われるようになり，デュアルスタックネットワークが一般的になると，フォールバック問題は顕著になると考えられる．ネットワーク管理者は，フォールバックが発生する可能性を考慮し，ネットワークの品質確保や，TCP Reset 実施などのワークアラウンドを用いて，ユーザに対する良好な通信環境の提供に留意する必要がある．

参考文献

[1] S. Deering, R. Hinden. “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, Dec 1998.

[2] R. Draves, “Default Address Selection for Internet Protocol version 6 (IPv6).”, RFC3484, Feb 2003

[3] 萩野純一郎，「IPv6 ネットワークプログラミ

ング」, ISBN : 4-7561-4236-2

[4] Carpenter, B. and K. Moore "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, Feb 2001

[5] R. Hinden, B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, Oct 2005.

[6] A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, Dec 1999

[7] M. Crawford, B. Haberman, Ed., "IPv6 Node Information Queries.", RFC 4620, Aug 2006

[8] A. Conta, S. Deering, Gupta, Ed.. "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, Mar 2006

[9] R. Braden, Ed.., "Requirements for Internet Hosts - Communication Layers.", RFC 1122, Oct 1989

[10] F. Gont, "TCP's Reaction to Soft Errors", < draft-ietf-tcpm-tcp-soft-errors>, Internet-Draft, Jun. 2007.

[11] "Summary and Status of Default Address Selection for IPv6", http://www.nttv6.net/dass/

[12] R. Draves, D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, Nov 2005