IPv6 Topics

IPv6とICMPv6

IPv4（Internet Protocol）には、補助プロトコルとしてICMP（Internet Control Message Protocol）が定義されている。IPv6にも同様に、IPv6コアプロトコルに対して、ICMPv6が存在する。ICMPは、送信したパケットに対するエラー通知や、ネットワークからの情報の取得などに利用されているが、現インターネットでは、セキュリティの強化などの目的から、ICMPをフィルタしていることも多い。しかしながら、IPv6はIPv4以上に、ICMPの機能を利用し、通信の制御を実施しているため、ICMPv6をフィルタしてしまうと、IPv6の通信に多大な影響を及ぼすことがある。

ICMPv4とICMPv6の違い

IPv4のICMPは、RFC792 にて規定されている。前述の、エラー通知での利用としては、IPパケットの転送や処理の際に障害が発生した場合、転送経路途中のルータやノードが、IPパケットの始点ノードにその障害の内容を報告するために使われる。元々のIPパケットを送出した始点ノードは、ICMPによって報告された障害の内容により、パケットを再送するか、通信を中止するか等の判断を実施する。RFC792にはいくつかのエラーメッセージが定義されているが、Source Quenchメッセージや、Redirectメッセージの一部など、セキュリティ上や機能上の問題から今日では実装されていないメッセージも多く存在する。また、情報取得の利用においては、ノードへの到達性の確認に今日でも多用されているICMP Echo/Echo Replyメッセージ（ping コマンドで使用される）が存在するが、それ以外のInformation Request/ Information Replyメッセージや、Timestamp Request/ Timestamp Replyメッセージは今日ではあまり利用されない。

ICMPv6では、ICMPv4の使用実績を考慮し、メッセージ種別の明確な分離、不要メッセージの削除などが実施されている。表1に、RFC2463“Internet Control Message Protocol（ICMPv6）for the Internet Protocol Version 6（IPv6）Specification”にて定義されているICMPv6のメッセージを示す。このRFCで規定されている以外にも、RFC2661“Neighbor Discovery for IP Version 6（IPv6）”（近隣探索プロトコル）やRFC2710“Multicast Listener Discovery（MLD）for IPv6”、RFC3810“Multicast Listener Discovery Version 2（MLDv2）for IPv6”、その他モバイルIP関連のRFC等で、追加のICMPメッセージが規定されている。

RFC 2461の近隣探索プロトコルは、IPv6の核となるプロトコルであり、IPv4におけるARP プロトコル（RFC826）と、ICMPルータ探索プロトコル（RFC1256）、ICMPリダイレクト（RFC792）の機能を併せ持ったものである。IPv6ノードは、以下の目的に「近隣探索（Neighbor Discovery）」を利用する。

- 同一リンク上に接続されている他のIPv6ノード（近隣ノード）のリンク層アドレスを得る。
- IPv6ノードがキャッシュしたリンク層アドレスが有効でなくたった場合にすぐにキャッシュをクリ

表1　ICMPv6のメッセージタイプ

ICMPエラーメッセージ（0～127）	
1	終点到達不可能
2	パケット過大
3	有効期間超過
4	パラメータ問題
ICMP情報メッセージ（128～255）	
128	エコー要求
129	エコー返答

IPv6 Topics

アする。
・ホストが、同一リンク上に存在し、パケットを中継してくれる近隣ルータを探す。
・近隣ノードが通信可能か、通信不可能かを能動的に把握する。
・リンク層アドレスの変更を発見する。

これらの機能は、すべてICMPv6を使用して実現されている。

ICMPのフィルタリング

前述のように、現在のインターネットでは、セキュリティ上の観点から、ICMPをフィルタすることが多いが、IPv4環境においても、ICMPのフィルタにより、通信不全に陥る例が存在する。図1に、ICMPがフィルタされた場合に通信ができなくなる例を示す。IPv6では、ノードにて、経路MTU探索を実装することが推奨されている。これは、IPv6では経路途中でパケットの分割を実施しないため、通信の際に最適な経路MTUを求める必要があるためである（IPv4でも、経路MTU探索を実装している場合には同様の問題が発生する。実際に、Windows等で問題が発生している）。ICMPがフィルタされると、経路途中にあるMTUの小さなリンクの存在を関知できず、通信に障害が発生することがある。この場合の典型的な例として、短いパケットは通るが、途中のMTU以上のパケットが通らないため、通信ができたりできなかったり、という事象が観測され、トラルシューティングが困難である場合が多い。

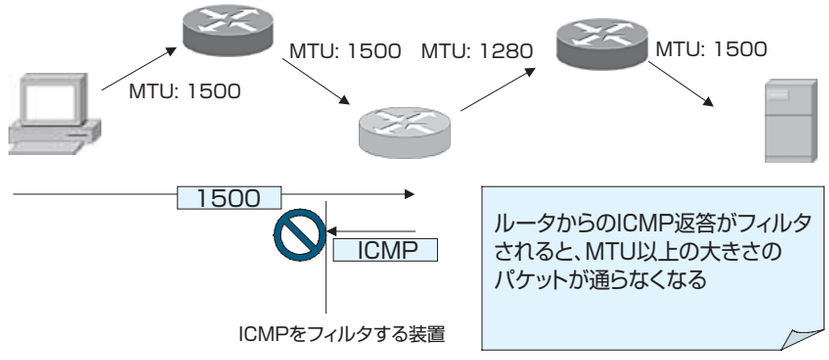

図1　ICMPのフィルタによる影響

また、IPv6ではICMPv6がその機能の重要な部分を担っているため、IPv4よりもICMPv6がフィルタされた影響は大きい。例えば、ノードでICMPv6をすべて受け付けないように設定すると、前述のIPv6近隣探索プロトコルのパケットも受け付けなくなる。IPv4のARP相当機能が動作しないため、結果として他のノードと全く通信ができなくなってしまう。特に、インターネットに更改しているノードや、組織外縁のルータでは、セキュリティ確保のためにこのような設定をしてしまうことがある。リンクローカルアドレスからのICMPは通信を許可する、等の設定をする必要がある。

IPv6におけるICMPv6フィルタのあり方については、IETFでも議論が進んでいる。IPv6ネットワークのオペレーションについて検討するv6opsワーキンググループで議論されている、“Recommendations for Filtering ICMPv6 Messages in Firewalls”（draft-ietf-v6ops-icmpv6-filtering-recs）では、現在IPv6で定義されているほとんどすべてのICMPメッセージに対して、フィルタに関連した扱いをどうすべきか、ということを詳述している。ICMPv6をフィルタする際には、よく考慮した上で実施することが必要である。

IPv4とIPv6の通信切り替え

今後増大していくであろう、IPv4とIPv6が混在した環境では特にICMPが重要な役割を果たす。

ユーザーがインターネット上の他ホストと通信する場合には、URL等でホスト名を指定し、DNS（Domain Name System）がホスト名をIPアドレスに変換する。最近のOSではDNSを用いてホスト名をアドレスに実施する際に、IPv4アドレスとIPv6アドレスの両方を問い合わせ、返答として両方のアドレスが得られた場合には、IPv6アドレスでの通信を先に試し、その後でIPv4アドレスの通信を実施するものが多い（図2）。IPv6ネットワーク接続性が十分な場合には、最初のIPv6通信が成功するため問題はない。しかしながら、IPv6接続性

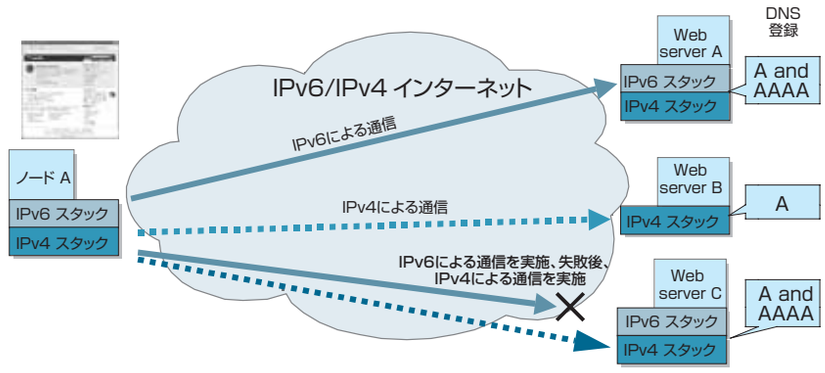

図2　IPv4／IPv6 通信切り替え

に異常があった場合には、失敗を検知した後にIPv4通信に切り替わる。この検知には、ICMPが利用される（上記、ICMPエラーの終点到達不可能メッセージが返答されることが多い）が、このICMPがフィルタされていると、始点ノードは通信エラーを検知することができない。WebブラウザのようなTCPベースのアプリケーションでは、通信のタイムアウトが発生するまで再送を繰り返すことになり、ユーザーは、Webページが表示されるまで、20秒以上も待たされることになる。

通信切り替え問題の実際

しかしながら実際のところ、ICMPv6の終点到達不可能メッセージが返答されたとしても、即座にIPv6通信からIPv4通信に切り替えを実施するOSは少ない。表2に、主なOSの通信切り替えにかかる時間の測定値を挙げる。ICMPエラーメッセージの返答があった場合の動作は、プロトコルごとに異なる。TCPの場合、ICMPメッセージへの動作は、RFC1122“Requirements for Internet Hosts – Communication Layers”にて定義されている。このRFCでは、ICMPをソフトエラー（回復する可能性のあるエラー。ホストへの経路情報の欠如（No route to host）、など）、ハードエラー（回復する可能性の少ないエラー。ノードでサービスが実行されていない（Port unreachable）、など）に分類しており、ハードエラーが返ってきた場合にはすぐにTCPセッションを切断するが、ソフトエラーの場合にはセッションを切ってはならない、と規定されている。

表2　通信切り替えにかかる時間

対象マシン（OS）	TCP [SYN]に対する回答パケット（None/ICMPv6タイプ・コード/TCP RST）		フォールバックに要した時間（秒）
Windows XP（SP2）	なし（何も回答しない）		22.868921
	1（Destination Unreachable）	0（no route to destination）	22.908757
		1（communication with destination administratively prohibited）	22.940496
		3（address unreachable）	22.914166
		4（port unreachable）	22.922729
MacOS aX Tiger	なし（何も回答しない）		149.575911
	1（Destination Unreachable）	0（no route to destination）	11.883733
		1（communication with destination administratively prohibited）	11.549623
		3（address unreachable）	11.843969
		4（port unreachable）	11.980887

IPv6環境での問題は、このRFC1122は非常に古く、IPv4のみを対象としているため、ICMPv6に関する記述が存在しないことである。また、この“ソフトエラー”、“ハードエラー”という分類自身が既に古く、現在のインターネット環境に合っていない、という指摘もある。これについては、現在IETFで議論されており、提案のドラフト（draft-ietf-tcpm-tcp-soft-errors、“TCP's Reaction to Soft Errors”）では、IPv6/IPv4デュアルネットワーク環境での状況を前提に、ソフトエラー相当のICMPメッセージでもTCPコネクションをすぐに切断することや、ICMPv6のエラーのソフト/ハード分類の考え方を述べている。最近のLinux等では、このドラフトを実装しているものも存在する。

IPv6ネットワークが一般的になるにつれて、ファイアウォールでのフィルタに関する問題や、IPv4/IPv6ネットワーク共存時の問題などが顕在化してきている。IPv6ネットワークを快適に使うために、IPv6の機能を理解し、適切なネットワーク運用管理を実施することが重要である。

[参考]
OSごとのTCP通信切り替え時間については、http://v6fix.net/docs/index.html の“IPv6/IPv4 fallback and DNS queries”に詳述されている。