

# Linux Kernel 2.6 の IPv6 プロトコル・スタック 詳解

## ICMPv6 の近隣探索処理

赤松 徹

第  
3  
回

今回は第3層受信処理を行う `ipv6_rcv()` 関数を中心に解説した。最後に ICMPv6 (Internet Control Message Protocol version 6) の場合は `icmpv6_rcv()` 関数に分岐することを確認した。今回は、ICMPv6 の近隣探索処理の内容に焦点を当てて解説する。(筆者)

### ICMPv6 パケット解析

IPv6 ネットワークの接続チェックのために、`std01.kic.ac.jp` から `std05.kic.ac.jp` 宛てに `ping6` コマンドを実行してみます(図1)。このとき `fe80::` で始まる IPv6 リンク・ローカル・アドレス宛てに `ping6` を発信するときは、`-I` で発信時に使用するインターフェース(`eth0` など)を指定します。

図1の結果を見ると、何msで返信を取得したかがわかります。そこで `std05` ホスト上で送受信する IPv6 パケット情報を `ip6tables` の `QUEUE` ターゲットを利用して取得しました(図2)。

図2(a)は IPv6 ヘッダの `nexthdr` 値が 58 なので、ペイロード上の情報は ICMPv6 です。ペイロード上の先頭4オクテットは、図3に示す ICMPv6 ヘッダの共通部分です。この type の値とカーネル内部で処理する名前との関連を図4に示します。type の値とカーネル内部で処理する名前との関連は `include/linux/icmpv6.h` と `include/net/ndisc.h` のヘッダ・ファイル内で定義しています。この type は 135 で code は 0 なので、近隣要請(`NDISC_NEIGHBOUR_SOLICITATION`)です。近隣要請は ICMPv6 に含まれます。

図2(b)は近隣要請に対する応答の近隣通知です(これも ICMPv6 に含まれる)。 `nexthdr` 値が 58 なので、ペイロードには ICMPv6 情報を運んでいます。ペイロード上の先頭4オクテットを確認すると、type が 136 で code が 0 なので近隣通知(`NDISC_NEIGHBOUR_ADVERTISEMENT`)です。

今説明したように近隣要請を発信して近隣通知を得る手順で、送信先のリンク・アドレスを取得したので、エコー要求パケットを発信できます。図2(c)は `nexthdr` 値が 58 なのでペ

イロード上には ICMPv6 情報を運んでいます。ペイロードの先頭4オクテットを図3の ICMPv6 ヘッダと照合すると、type が 128 で code が 0 なので、`std01` から `std05` へのエコー要求(`ICMPV6_ECHO_REQUEST`)です。

図2(d)はエコー要求に対するエコー応答です。繰り返し説明したので、IPv6 パケットの確認方法を理解できたと思います。IPv6 ヘッダの `nexthdr` 値が 58 なので、ペイロードは ICMPv6 を運んでいます。ペイロード上の先頭4オクテットを確認すると、type は 129 で code が 0 なのでエコー応答(`ICMPV6_ECHO_REPLY`)です。

### icmpv6\_rcv() 関数の処理

それでは `ping6` を実行してネットワーク接続を確認したときに、カーネル内部でどのような処理がなされているかを確認しましょう。

受信した ICMPv6 パケットが第4層に到達したとき、最初に処理される関数は `icmpv6_rcv()` であることを前回確認しました。この関数はリスト1に示すように、`net/ipv6/icmp.c` ファイルの584行目以降にあります。

ICMPv6 パケットを受信したので、594行目でカウンタを(+1)します。この情報は `/proc/net/snmp6` ファイルに記録されます。カウンタ名(`ICMP6_MIB_INMSGS`)とファイルに記録される項目名との関係は、`net/ipv6/proc.c` ファイルの98行目以降に定義されています。

```
net/ipv6/proc.c
98  SNMP_MIB_ITEM("Icmp6InMsgs",
                                ICMP6_MIB_INMSGS),
```

```
# ping6 -c 1 -I eth0 fe80::200:1aff:fela:a8c
PING fe80::200:1aff:fela:a8c(fe80::200:1aff:fela:a8c) from fe80::200:1aff:fela:9fa eth0: 56 data bytes
64 bytes from fe80::200:1aff:fela:a8c: icmp_seq=0 ttl=64 time=1.36 ms

--- fe80::200:1aff:fela:a8c ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.369/1.369/1.369/0.000 ms, pipe 2
```

図1 std01 から std05 へ ping6 で接続確認したところ

