



@IT > クラウド > Windows Server Insider > 第12回 TCP/IPプロトコルを支えるICMPメッセージ：...

# 第12回 TCP/IPプロトコルを支えるICMPメッセージ

(2/3 ページ)

2003年06月13日 00時00分 公開

[デジタルアドバンテージ, 著]

印刷

通知

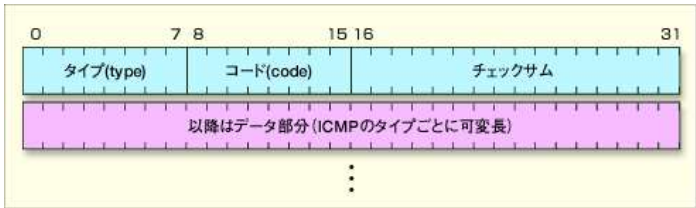
見る

Share

18

## ICMPメッセージの構造

以下にICMPパケットの構造を示しておく。実際には、この直前にIPパケット（のヘッダ部分）があり、ICMPの通信先や通信元の情報は、そこから得ることになる。



ICMPパケットの構造  
ICMPの最小サイズは4bytes + メッセージごとのオプション・サイズとなっている。どのメッセージでも、先頭の4bytesは同じ形になっている。チェックサムはIPヘッダなどと同様に、「1の補数」形式で計算する。

ICMPパケットには、その機能によって何種類かのパターンがあるが、基本的な構造はこのように、1byteの「タイプ（機能コード）」、1byteの「コード（補助的な機能コード）」、そして2bytesの「チェックサム」フィールドから構成されている。そして必要に応じて何bytesかの追加データ・フィールドが続くことになっている。チェックサムはIPヘッダなどと同じように、「1の補数」形式で計算される。「1の補数」演算については連載第10回の「1. IPパケットの構造」を参照していただきたい。

先頭にある「タイプ」フィールドは、ICMPメッセージの機能や種類を表す。場合によってはさらに「コード」フィールドを使って、より細かな機能の指定を行うこともある。

実際に利用可能なICMPの一覧は次のとおりである。ただし、すべてのノードが、すべての種類のタイプをサポートしているわけではなく、非ルータのノード（つまり一般のクライアント・ノード）では、限定的ないくつかのタイプしかサポートされていない。

タイプ	機能
0	エコー応答 (echo reply)
3	あて先不達 (destination unreachable)
4	ソース・クエンチ (source quench、送信元抑制)
5	リダイレクト要求 (redirect、経路変更要求)
8	エコー要求 (echo request)
11	時間超過 (time exceeded)
12	パラメータ異常 (parameter problem)
13	タイムスタンプ要求 (timestamp request)
14	タイムスタンプ応答 (timestamp reply)
15	情報要求 (information request)
16	情報応答 (information reply)
17	アドレス・マスク要求 (address mask request)
18	アドレス・マスク応答 (address mask reply)

ICMPメッセージの一覧  
ICMPメッセージの一覧はRFC792とRFC950（アドレス・マスク）で定義されている。

### ホワイトペーパー

- インターネットの急な不調は「アクセス集中(輻輳)」のせい? 有効な回避策は
- 検知してからどうするか!? 標的型サイバー攻撃における内部対策の提案
- ネットワーク製品の導入に関する読者調査レポート(2014年12月)
- もう「Wi-Fi 7」時代? 無線LANの気になる進化

### スポンサーからのお知らせ

- PR -

重要なのは発展性 なぜ今、“ストレージ”に注目が集まっているのか

「ネットワークが分からない」状態からでも丸ごとサポート

### Special

- PR -


- 複数ベンダーの「継ぎはぎSASE」で生じる課題、どうすれば解決できるのか?
- データは「守りながら活用する時代」に
- オンプレのハードウェアも「サブスク」の時代へ コストや契約はどう変わる?

データ部分の使い方はICMPメッセージごとに異なる。ICMPエコー・メッセージでは、ユーザー（アプリケーション）が指定したデータを格納しているが、エラーを返すメッセージでは、エラーの元となった（エラーを引き起こした）IPパケットの先頭部分（IPヘッダ+ユーザー・データの一部）の内容をデータとして格納していることが多い。このデータ部分を解析することにより、どのIPパケットがエラーを引き起こしたのかを調べたり、エラーの発生原因などを詳しく調査したりできるようになっている。ただしOS自体には、このようなICMPのエラー・メッセージを解析するような機能は含まれておらず、一般的にはパケット・アナライザ（ネットワーク上のパケットをキャプチャして解析するツール）などを使って技術者が解析することになる。

以下、それぞれのICMPメッセージについて詳しく見ていこう。

タイプ8／0—ICMPエコー要求／エコー応答

「ICMPエコー」は、指定されたエコー・データ・パケットを、2つのTCP/IPノード間で送受信するためのメッセージである。ICMPエコーの送信元が送ったデータ・パケットが相手のノードに届くと、そのデータがそっくりそのまま元のノードへと送り返されてくる。この応答操作ではアプリケーションは介在せず、TCP/IPのプロトコル・スタック自身が応答処理を行う。パラメータとなるデータをそのまま送り返すので「エコー」と呼ばれており、TCP/IPのプロトコル・スタックが稼働しているかどうかを調べるために使われる。TCP/IPをサポートしているノードは必ずこの機能を実装することが求められており、ノードの動作状態を調査するためには欠かせない機能である。一般ユーザーが利用するpingコマンドは、このICMPエコー機能を使って実現されている。

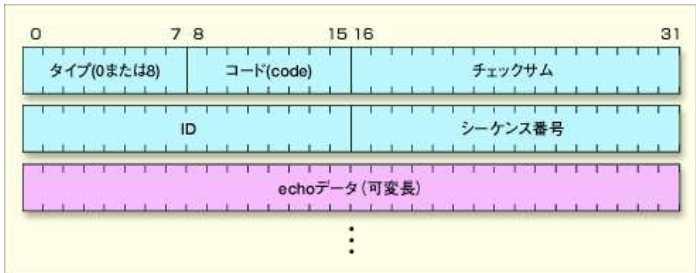


Special

中堅中小企業の“ネットワーク課題”はこれで解決！

- PR -

以下に、ICMPエコーのパケット構造を示しておく。



**ICMPエコー・パケットの構造**  
ICMPエコーには「要求」と「応答」の2種類があり、先頭byteの「タイプ」フィールドで区別する。コード・フィールドは未使用。最初にパケットを送信する側が「要求」を送ると、受信した側が「応答」パケットに変更して、送信元へ返信する。このパケットの前には、IPヘッダ、およびイーサネットなどのデータリンク層のヘッダが存在する。データ部分は可変長であり、最大サイズはIPパケットの最大長に限定される。データ部分の長さは、IPパケットの全体長から自動的に計算される。

先頭にある「タイプ」フィールドには「エコー要求（8）」か「エコー応答（0）」がセットされる。最初にエコー要求を出す方が、タイプ・フィールドに「エコー要求（8）」をセットしてパケットを送信すると、受信した側では、タイプを「エコー応答（0）」に変えて元のパケットをそのまま返信する。コード・フィールドはこのICMPメッセージでは使用されない（0が入っている）。

「ID」と「シーケンス番号」は、ICMPエコー・メッセージを利用するアプリケーションが自由に利用できるフィールドである。通常は、エコー・メッセージを送信する側において、送信したパケットを一意に識別できるような数値をセットする。エコー・メッセージでは、これらのフィールドの内容もそのまま変更せずにパケットを送り返すた



「ほとんど誰も見ていない」社内ポータル、どう変えるべき？  
New!



ローコードツールの現在地。AI、機械学習とのシナジーで新たな価値を生み出す  
New!



「守る」だけでは不十分 今どきのストレージには何が必要？



社内ルールだけでは限界 有名無実化した「ローカル保存禁止」にどう対応？



「ネットワークが分からない」状態からでも丸ごとサポート  
New!



NTTデータと日本IBMがタッグ！AIは仕事をどう変える？

@IT Special ^

Windows Server Insider 記事ランキング

- 本日

月間
- Excel（エクセル）で日付から自動的に曜日を入力する
- 【Excel】重複データを色付けして瞬時にダブりをチェックする
- 【Excel】パスワードロックを強制的に解除する方法
- TCP/IP通信の状態を調べる「netstat」コマンドを使いこなす【Windows OS】
- Windows OSのdirコマンドでファイル名の一覧を取得する
- システム要件を満たさないPCをWindows 11 2023 Update（23H2）にアップデートする方法
- 【Windows 10／11】えっ、UTF-8じゃなくてShift-JISで？ お手軽文字コード変換方法まとめ
- PDFファイルにキーボードから直接文字入力する方法【本家Acrobat Reader編】
- Excelの落とし穴「先頭のゼロ（0）」問題の対処法
- 【Windows 10／11】PCが数分で勝手にスリープするのを防ぐ

ランキングをもっと見る

あなたにおすすめの記事

- PR -



オンプレのITインフラを「サブスク」で利用できるサービスは何がスゴイのか？

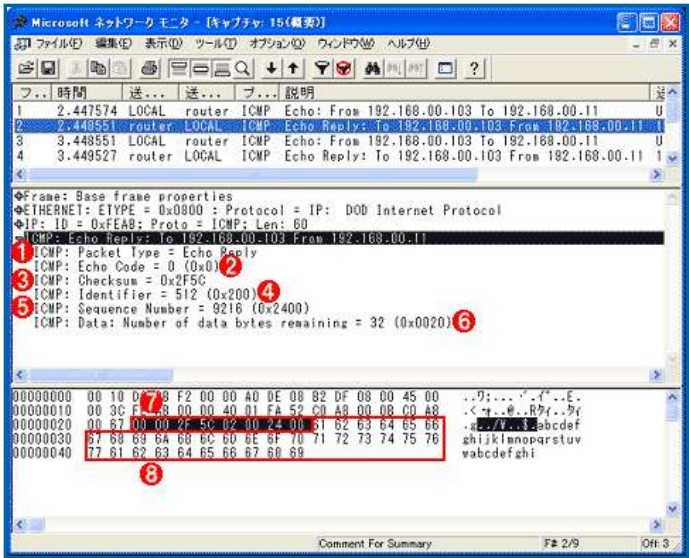


自分が作ったアプリがスマホで動くさまを見ると、学生の目が輝きます  
New!

め、受信した側でこれらのフィールドの内容を調べることで、どのエコー要求に対する応答であるかを識別することができる。同時に複数の要求パケットを送信して、その応答時間が大きくずれているような場合とか、同時に複数のユーザーがpingコマンドを実行した場合でも、どの要求パケットに対する応答であるかが分かるようになる（パケットを送信するたびに異なる値をセットしておく）。

「echoデータ」フィールドには、ICMPエコー・メッセージを利用するアプリケーションが何らかの値をセットしておく（データの内容は何でもよい）。一般的には、バイナリ・データ（0x00～0xffまでを順番に1ずつ変更したもの）が使われることが多い。

以下に、実際のpingコマンドの例を示しておく。データ部には、文字列のようなデータ（実際には+1ずつ値を変えたバイナリ・データ）が入っていることが分かるだろう。



ICMPエコーの例

Windows XPシステム上でpingコマンドを実行した場合の応答パケットの例。アプリケーション（この場合はpingコマンド）が指定したバイナリ・データが相手に送られ、それがそのまま返信されている。

- (1) ICMPメッセージのタイプ。0x00はICMPエコー応答。
- (2) コードは未使用（0x00になっている）。
- (3) ICMPパケットのチェックサム。1の補数演算が使用されている。
- (4) この値は、常に同じ値になっているようである。
- (5) シーケンス番号。1パケット送信ごとに「+0x0100」されているようである。これによって、echo要求とその応答を判別している。
- (6) データ部分の内容は任意。デフォルトでは32bytes。
- (7) ICMPのエコー応答のヘッダ部分。
- (8) この例では、データ部分は'a'から始まるバイナリ・データになっている。1byteごとに+0x01されている。

ICMPエコーで1度に送信できるデータのサイズは、IPパケットの最大長に制限される（ICMPエコー・パケット自体にはデータ長を表すフィールドは用意されていない）。そのため、例えば64Kbytesといった大きなサイズのエコー・パケットを送信することも可能であるが、現実のTCP/IPネットワークでは、このような巨大なサイズのエコー・パケットは許可していないことが多い。特にファイアウォールが装備された環境では、フラグメンテーションが必要なサイズのIPパケットは許可されていないことがある。IPフラグメンテーションを処理するためには、IPパケット全体を再構築するために一時的にバッファを用意し、ばらばらに到着したフラグメントを順次組み合わせる必要があるが、このためには全部のパケットが到着するまで、TCP/IPのプロトコル・スタック内にそれらを保持しておかなければならない。だがこのような（不完全な）フラグメンテーション・パケットをわざと大量に送りつけると、プロトコル・スタックに負荷がかかり、システムが不安定になる可能性がある。このようなDoS攻撃を避けるため、ファイアウォールの設定によっては、フラグメンテーションが必要なIPパケットの受信はすべて拒否することがある。

このような事情があるため、pingで利用可能な最大データ長は、ネットワークの設定によって変わることになる。もしフラグメンテーションが許されないとすると、ICMPエコーのパケット・サイズは1つのイーサネット・フレームなどに収まるサイズに制限され



“企業が重視するポイント”に合わせたバックアップソリューションとは

@IT Special

ミドルの転職・AMBIの人気コンテンツ - PR -



若手7割がスタートアップ転職に意欲 | AMBI (アンビ)



あなたの職務適性が15分でわかる | AMBI (アンビ)

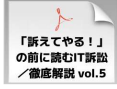


官公庁関連の厳選求人、多数掲載中！「ミドルの転職」

@IT eBook



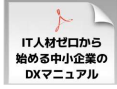
解決！Python CSVファイル編



誰か、要件追加を止めてくれ！——「旭川医大の惨劇」徹底解説



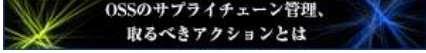
目指せ、共有フォルダ管理の達人！ Windowsファイル共有を“極める”ためのPowerShellコマンドレット基本集



IT人材ゼロでDX!? お悩み中小企業のためのDX推進が分かる無料の電子書籍とは

一覧ページへ

注目のテーマ



システム開発ノウハウ【発注ナビ】 - PR -



「AI開発」でおすすめの25社【2023年版】



Excelではもう限界！2万点以上の在庫管理をシステムで解決



受注ゼロから一転、開発会社が2000万円の案件を獲得できた理由



ることになる。一般的なLAN環境で広く使われているイーサネットでは、最大ユーザ・データ・サイズは1500bytesまでとなっているので、ここからIPヘッダのサイズ（最小で20bytes）とICMPパケットのサイズ（ヘッダ部分だけで8bytes）を引くと、有効なエコー・データの最大サイズは1472bytesとなる。またDSL回線でPPPoEなどが利用されていると、さらに小さなMTUサイズしか利用できないので、もっと小さなサイズのエコー・データしか利用できないことになる。例えばPPPoEを利用するNTTのフレッツADSLなどでは、MTUサイズは1454bytesに制限されているので、フラグメントなしに利用可能なICMPエコーのデータ長は、 $1454 - 20 - 8 = 1426$ bytesまでとなる。

以下で実際にMTUサイズとエコー・データのサイズについて見てみよう。

すでに述べたように、ICMPエコーを利用するためには、pingコマンドを使う。pingコマンドにはいくつかオプションがあるが、「-f」オプションを使うと、フラグメンテーションを許可しない、というモードになる。具体的には「-f」オプションを使うと、[第10回](#)で解説した、IPヘッダ中の「DF (Don't Fragment) ビット」がオンになり、フラグメンテーションが禁止される。もしフラグメンテーションが必要なくらい大きなデータを送信しようすると、エラーが報告される。

まずはローカルのイーサネットLAN上でpingを実行してみる。この場合は、フラグメントなしに送信できるエコー・データの最大長は1472bytesのはずである。1472bytesと1473bytesの2通りでpingを実行してみよう。「-f」はフラグメントを許可しないという設定、「-n 1」は1パケットだけ送信するという設定、そして「-l 1472」はエコー・データのサイズを1472bytesにするという設定である。

```
C:\>ping -f -n 1 -l 1472 192.168.0.1 .....データ長は1472byte

Pinging 192.168.0.1 with 1472 bytes of data:

Reply from 192.168.0.1: bytes=1472 time=5ms TTL=64 .....正しく送信できた

Ping statistics for 192.168.0.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 5ms, Average = 5ms

C:\>ping -f -n 1 -l 1473 192.168.0.1 .....データ長は1473byte

Pinging 192.168.0.1 with 1473 bytes of data:

Packet needs to be fragmented but DF set.
↑↑途中のルータから、エラーで送信できないという応答があった
Ping statistics for 192.168.0.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

これから分かるように、データ長が1473bytesでは「Packet needs to be fragmented but DF set.（フラグメンテーションが必要なパケット・サイズであるが、DFフラグがセットされていたので送信できない）」というエラーになっている。つまりこのLAN上では、最大MTUは1500bytes（エコー・データのサイズは1472bytes）までということが分かる。

次は、PPPoEを使ってインターネット接続されている環境において、インターネット上のホストに対してpingを実行してみる。この場合の最大エコー・データ長は1426bytes（ $1454 - 20 - 8 = 1426$ bytes）のはずである。

```
C:\>ping -f -n 1 -l 1426 202.XX.XX.XX .....データ長は1426byte

Pinging 202.XX.XX.XX with 1426 bytes of data:

Reply from 202.XX.XX.XX: bytes=1426 time=17ms TTL=246 .....正しく送信できた

Ping statistics for 202.XX.XX.XX:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 17ms, Average = 17ms

C:\>ping -f -n 1 -l 1427 202.XX.XX.XX .....データ長は1427byte
```



```
Pinging 202.XX.XX.XX with 1427 bytes of data:
```

```
Reply from 210.150.YY.YY: Packet needs to be fragmented but DF set.
```

↑↑途中のルータから、エラーで送信できないという応答があった

```
Ping statistics for 202.XX.XX.XX:
```

```
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

エコー・データのサイズを1427bytesにしてみると、途中のノード（この場合は、インターネット接続に利用しているルータ：210.150.YY.YY）から、DFフラグがセットされているのでフラグメンテーションができない、というエラーが戻ってきている。つまり、インターネットへ接続する経路の途中に、MTUが1454bytesのネットワークが存在しているということが分かる。

Windows OS自体はもっと長いICMPエコー・パケットが利用できるが（pingコマンドでは最大で65,500bytesまでのデータ長が指定可能）、このように途中で通過するルータやファイアウォールなどの制約を受けて、実際にはもっと小さなサイズしか利用できないことも多い。

#### ICMPメッセージ (2)

[前のページへ](#)[1](#) | [2](#) | [3](#)[次のページへ](#)

Copyright© Digital Advantage Corp. All Rights Reserved.

- PR -

**C-Native**  
**クラウドシフトへの第一歩は、「C-Native」から**  
伴走型支援    パッケージプラン    短期導入

**CTC**  
C-Native Transformation Service

## 基礎から学ぶWindowsネットワーク 連載一覧

全 23 回

新しい連載記事が 9 件あります

第14回 [信頼性のある通信を実現するTCPプロトコル（その1）](#)

第13回 [データグラム通信を実現するUDPプロトコル](#)

第12回 **TCP/IPプロトコルを支えるICMPメッセージ**

第11回 [MACアドレスを解決するARPプロトコル](#)

第10回 [IPパケットの構造とIPフラグメンテーション](#)

過去の連載記事が 9 件あります

## Special

- PR -



「守る」だけでは不十分。今どきのストレージには何が必要？



ローコードツールの現在地。AI、機械学習とのシナジーで新たな価値を生み出す **New!**



オンプレのハードウェアも「サブスク」の時代へ。コストや契約はどう変わる？



データは「守りながら活用する時代」に



社内ルールだけでは限界 有名無実化した「ローカル保存禁止」にどう対応？



NTTデータと日本IBMがタッグ！ AIは仕事をどう変える？



「ほとんど誰も見ていない」社内ポータル、どう変えるべき？ **New!**



中堅中小企業の“ネットワーク課題”はこれで解決！ **New!**

[@IT Special](#)へ

この記事に関連する製品／サービスを比較（キーマンズネット）

既存のネットワーク構成とマッチする？『WAN高速化』製品の選び方  
まずネットワークの性質を十分に見極めよう！『ネットワーク管理』製品比較  
信頼性や可用性に対する取り組みは？『ネットワークスイッチ』製品比較  
L4負荷分散とL7負荷分散どちらを重視？『ADC／ロードバランサ』製品一覧  
構築したいネットワーク要件で大きく変わる『ルーター』の選び方

印刷

通知

見る

Share

18

- @ITについて
- お問い合わせ
- 広告について
- 採用広告について
- 利用規約
- 著作権・リンク・免責事項
- サイトマップ

- RSSについて
- @ITのRSS一覧

- アイティメディアIDについて
- アイティメディアIDとは

メールマガジン登録

@ITのメールマガジンは、もちろん、すべて無料です。ぜひメールマガジンをご購読ください。

申し込みページへ

ITmediaはアイティメディア株式会社の登録商標です。

[メディア一覧](#) | [公式SNS](#) | [広告案内](#) | [お問い合わせ](#) | [プライバシーポリシー](#) | [RSS](#) | [運営会社](#) | [採用情報](#) | [推奨環境](#)