

*ezTCP series*

T C P / I P ネットワークプロトコルモニタ

---

# e z M O N I T O R

---

取り扱い説明書

第2版 2002/12/27

**ALPHA PROJECT CO.,LTD**

## e z M O N I T O R 取り扱い説明書

このたびは、TCP/IP ネットワークプロトコルモニター「e z M O N I T O R」をお買いあげ頂きまして誠に有り難うございます。本製品をお役立て頂くために、本マニュアルを十分お読み下さいますようお願いいたします。  
今後共、弊社製品をご愛顧賜りますよう宜しくお願いいたします。

### 梱包内容をご確認ください

・プログラム / マニュアルディスク	× 1 枚
・ e z M O N I T O R のご使用条件	× 1 枚

本製品に含まれるソフトウェア及び電子文書の著作権は全てアルファプロジェクトが保有しています。  
無断で転載または複製することは堅くお断りいたします。

本製品の内容及び仕様は予告なしに変更されることがありますのでご了承ください。

本製品は万全の注意を払って製作されていますが、万一初期不良品であった場合、お買い上げ頂いた販売店へ保証書を添えてご返却ください。（弊社より直接お買い上げのお客様については、出荷時に全て登録済みとなっております。）  
保証内容、免責等につきましては、添付の保証書をご覧ください。

本書内で使用されている製品名は各社の商標です。

マニュアルの閲覧には、Adobe 社の AcrobatReader®が必要です。

# 目 次

## 1 . 製品概要

1

1 . 1	概要	1
1 . 2	機能及び特長	1
1 . 3	動作環境	2

## 2 . 機能説明

3

2 . 1	画面構成	3
2 . 2	フィルタリング機能詳細	8
2 . 3	ファイル保存機能	11
2 . 4	ファイル出力機能	12
2 . 5	メモリサイズについて	12

## 3 . チュートリアル

13

3 . 1	パケットのキャプチャ例	13
-------	-------------	----

## 4 . トラブルシューティング

9

1

4 . 1	トラブルシューティング	19
-------	-------------	----

## 4 . 製品サポートと使用上の注意

20

5 . 1	製品サポートのご案内	20
5 . 2	使用上の注意	20

---

## 1. 製品概要

### 1.1 概要

近年はネットワークの普及が進み、あらゆる用途においてネットワーク対応が求められるようになりました。しかし、ネットワーク上に流れるデータは膨大かつ種類も様々でありネットワーク対応製品の開発には多大な労力と時間が必要となります。

ezMONITORは、TCP/IPネットワークプロトコルモニタで、簡単にネットワーク上のデータをモニタリングすることができます。設定も簡素化されており、リアルタイムに状況が判断できる為、さまざまなネットワーク機器の開発を効率化することができます。

### 1.2 機能及び特長

#### 1) リアルタイムな監視が可能

ezMONITORはネットワーク上に流れるパケットを即時に表示できます。  
その為、リアルタイムなパケットの流れを監視することができ、正確なネットワークの状態が取得できます。

#### 2) 複数のプロトコルに対応

ezMONITORはTCP/IP、UDP、ICMPに対応しています。  
これらのプロトコルは現在のネットワークのほとんどに使用されているため、一般的なネットワーク機器であれば問題なく使用できます。

#### 3) 2種類のフィルタリング機能

ezMONITORはキャプチャ用と表示用の2種類のフィルタ設定が可能です。  
これにより必要なパケットのみを監視でき、さらに条件を絞り込んで表示できる為状況に応じたパケットの状態を知ることが可能です。

#### 4) キャプチャしたデータをファイルに保存

ezMONITORはキャプチャしたパケットをファイルに保存することができます。  
ファイルフォーマットはヘッダ付きバイナリ、ヘッダ無しバイナリ、ASCII形式と選択できるため目的に応じた使い方ができます。

#### 5) 長時間のパケットの記録が可能

ezMONITORは通常メモリ上にパケット情報を格納しますが、キャプチャしたパケットを直接ファイルに格納することも可能です。この機能により長時間かつ大量のパケットを記録することが可能となります。

### 1.3 動作環境

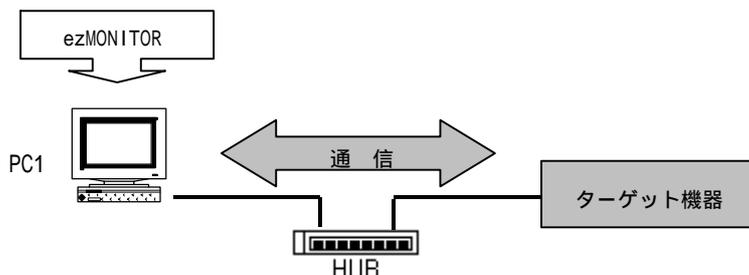
表 1.3 - 1 動作条件

機能	詳細
対応PC	Windows 95、98、Me、Windows 2000が動作する PC / AT互換機
CPU	Pentium 300MHz 以上
メモリサイズ	64 MByte以上 (128 MByte以上を推奨)
ネットワークアダプタ	NDIS対応ネットワークアダプタ
対応OS	Windows 95、98、Me、Windows 2000

Windows 2000ではMACアドレスの表示やフィルタリングに制限があります。

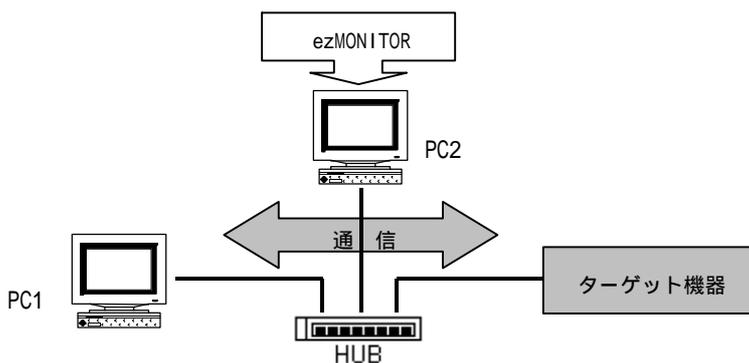
図 1.3 - 1 ezMONITORの接続例

自PCの通信をモニタする場合



PC1とターゲット機器との通信データを、PC1でモニタします。

他の機器間の通信をモニタする場合



PC1とターゲット機器との通信データを、PC2でモニタします。

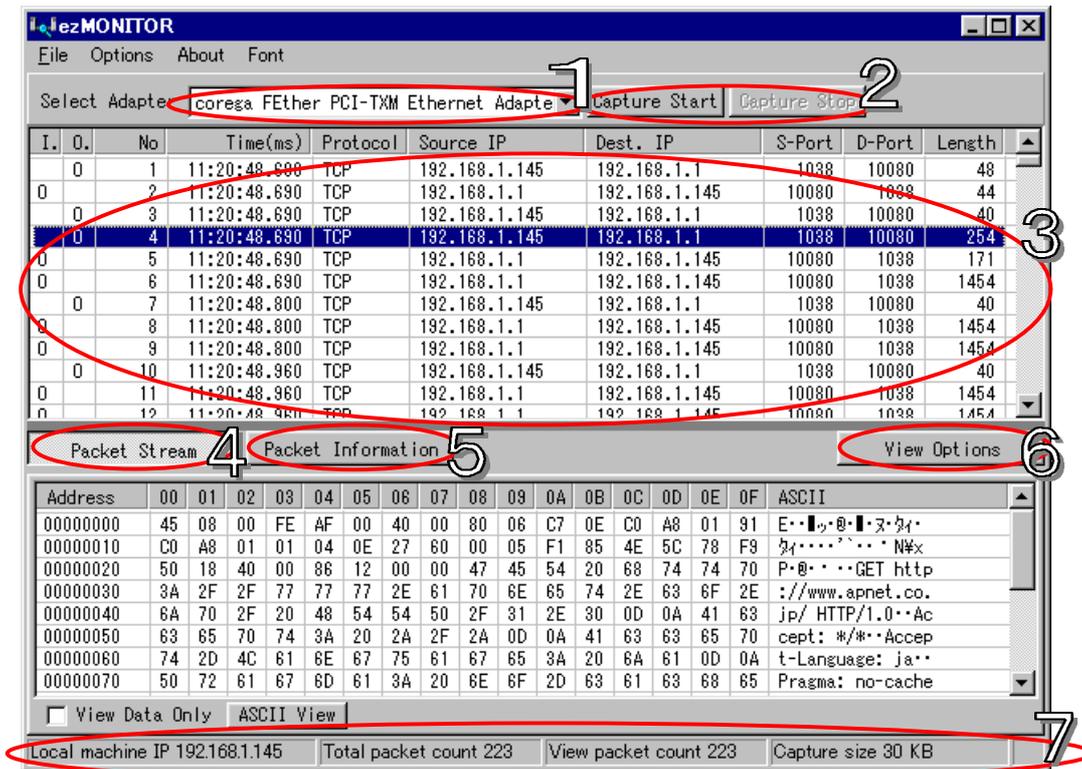
この方法ではHUBはスイッチング機能の無いもの(リピータHUB / シェアードHUB)に限ります。

## 2 . 機能説明

本章では、ezMONITOR の各画面について説明します。

### 2 . 1 画面構成

図 2 . 1 - 1 ezMONITORメイン画面



Select Adapter	キャプチャを行うネットワークアダプタを選択します。
Capture Start、Capture Stop	キャプチャの開始、停止を行います。
Packet List	キャプチャしたパケットの一覧を表示します。各項目は以下の通りです。
I n	基準となる I P に対しての入力
O ut	基準となる I P からの出力
No	キャプチャされたパケットの番号
Time(ms)	キャプチャされた時刻
Protocol	パケットのプロトコル
Source IP	発信元 I P アドレス
Dest. IP	送信先 I P アドレス
S-Port	発信元ポート番号
D-IP	送信先ポート番号
Length	パケット長

Packet stream 上のパケットリストで選択されたパケットをバイナリ形式(右)とASCII形式(左)で表示します。

View Data Only ここをチェックした場合、パケットのデータ部分のみを表示します

ASCII View データ領域をテキスト(ASCII)形式で表示します。

テキスト(ASCII)表示が不可能なデータが含まれている場合、正常に表示できない場合があります。

図 2 . 1 - 2 パケット表示部

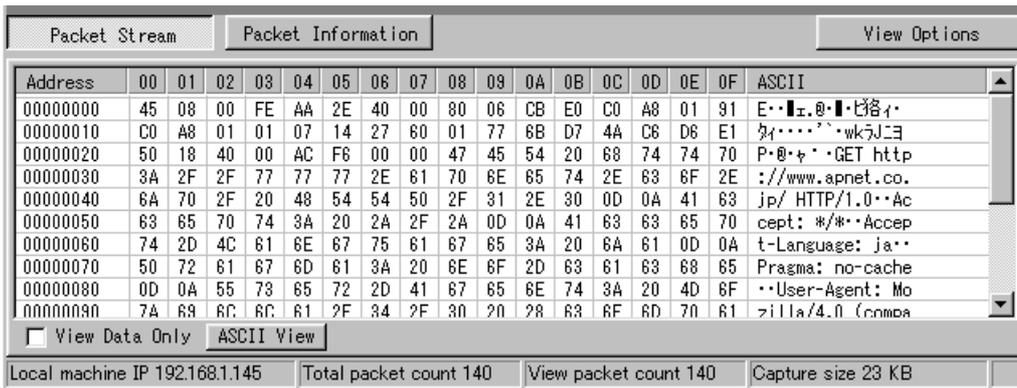


図 2 . 1 - 3 View Data Only 表示画面

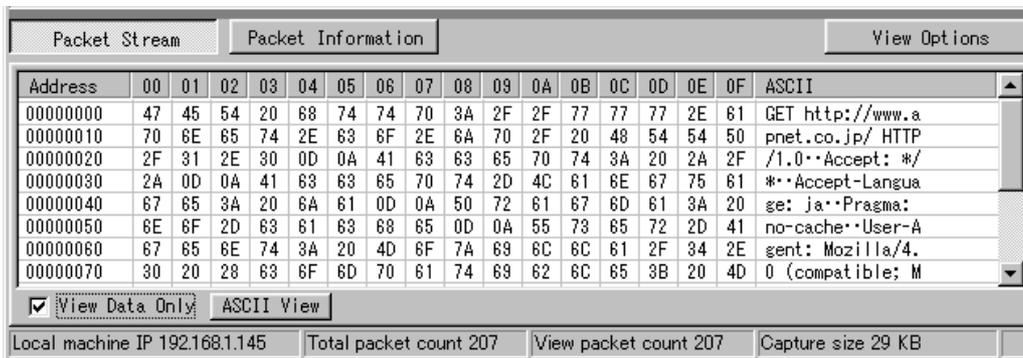
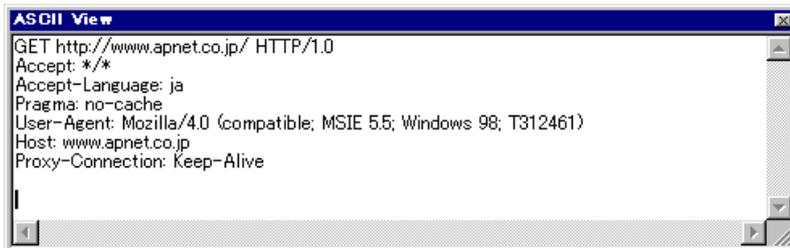


図 2 . 1 - 4 ASCII View 表示画面



Packet Information	パケットをバイナリ形式（右）とASCII形式（左）で表示します。
Time(ms)	パケットが取得された時間
Source Mac Address	発信元MACアドレス
Destination Mac address	送信先MACアドレス
Ethernet type	パケットの種類
IP Version	IPのバージョン
Length	パケットのサイズ
Protocol	プロトコル
Source IP	発信元IPアドレス
Destination IP	送信先IPアドレス
Source port	発信元ポート番号
Destination port	送信先ポート番号

Windows2000 では表示されません

図 2.1 - 5 Packet Information 表示画面

Data Name	Description
Time	15:50:25.890
Source Mac Address	00:90:99:22:F9:7F
Destination Mac Address	00:00:E2:0D:37:42
Ethernet Type	0800
IP Version	4
Length	254
Protocol	TCP
Source IP	192.168.1.145
Destination IP	192.168.1.1
Source Port	1812
Destination Port	10080

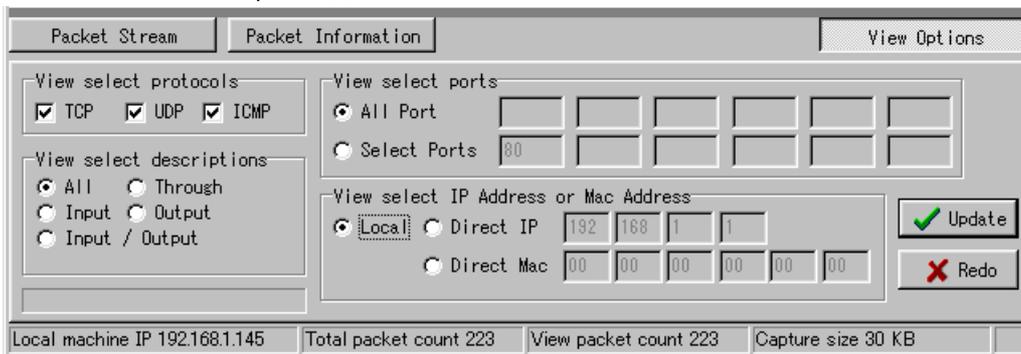
Local machine IP 192.168.1.145    Total packet count 140    View packet count 140    Capture size 23 KB

View Options	Packet List に表示するパケットの種類を選択します。 各設定は「Update」ボタンを押すことにより反映されます。
View select protocols	表示を行うプロトコルを選択します。
View select Direction	表示を行うパケットの方向を選択します。
View select Ports	表示を行うポート番号を選択します。 入力できる数値は 10 進数で 0 ~ 65535 までです。
View select IP address or MAC address	表示の基準となる IP アドレス又は MAC アドレスを選択します。IP アドレスは 10 進数で、MAC アドレスは 16 進数で入力してください。
Update	上記で変更された設定値を実際のパケットリストの表示に反映させます。表示パケット数が多い場合には時間がかかりますので注意してください。また、キャプチャ中に Update を行うとパケットを取りこぼす可能性があります。
Redo	変更された設定値を元に戻します。設定値は以前 Update が押された時点のものに戻り、パケットリストの表示内容は変更されません。

Windows2000 では MAC アドレスの選択はできません。

各項目の設定値については 2 . 2 フィルタリング機能詳細を参照してください。

図 2 . 1 - 6 View Option 表示画面



Capture Status	現在のキャプチャ状況を表示します。
Local Machine IP	ezMONITOR を実行している PC の IP アドレスを表示します。
Total Packet Count	ezMONITOR が取得したパケット数を表示します。
View Packet Count	ezMONITOR の Packet List に現在表示しているパケット数を表示します。
Capture Size	ezMONITOR が取得したパケットの総容量を表示します。

図 2 . 1 - 7 Capture Status 表示

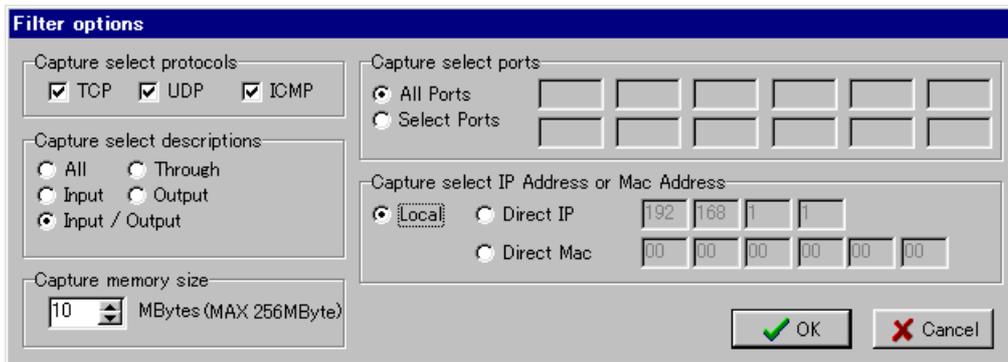


Filter Options	キャプチャするパケットの条件を設定します。 メニューの「Options」「Filter Options」にてダイアログが開きます。
Capture select Protocols	キャプチャを行うプロトコルを選択します。
Capture select Direction	キャプチャを行うパケットの方向を選択します。
Capture select Ports	キャプチャを行うポート番号を選択します。 入力できる数値は10進数で0~65535までです。
Capture select IP address or MAC address	キャプチャの基準となるIPアドレス又はMACアドレスを選択します。IPアドレスは10進数で、MACアドレスは16進数で入力してください。
Capture Momory size	キャプチャデータを確保するメモリサイズを指定します。

Windows2000ではMACアドレスの選択はできません。

各項目の設定値については2.2フィルタリング機能詳細を参照してください。

図2.1-8 Filter Options表示画面



## 2.2 フィルタリング機能詳細

ezMONITORは、パケットフィルタリング機能を備えており、この機能によりネットワークに流れる大量のデータから目的のデータだけを効率よく抽出することができます。

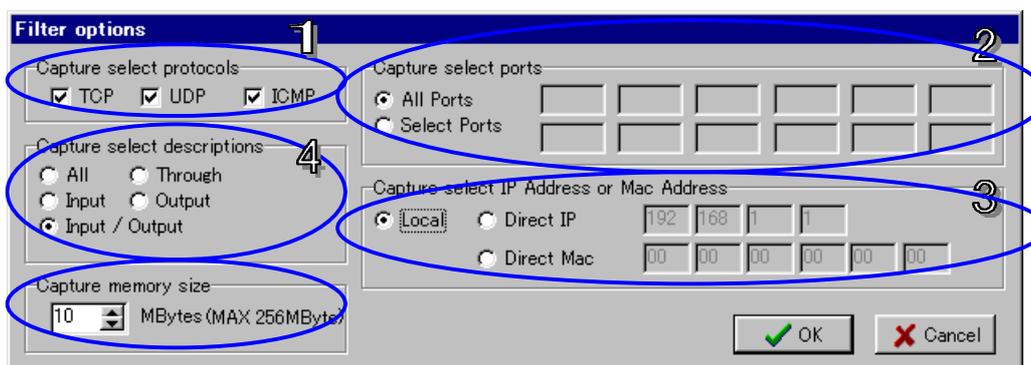
フィルタの設定にはキャプチャ用(Filter Options)と表示用(View Options)の2種類のフィルタ設定があります。

キャプチャ用フィルタはPCに流れてくるパケットをezMONITORで検出する為の条件を設定します。

表示用フィルタはその検出されたパケットの表示条件を設定するものです。

### 2.2.1 キャプチャ用フィルタの設定 (Filter Option)

図 2.2 - 1 Filter Options 表示画面

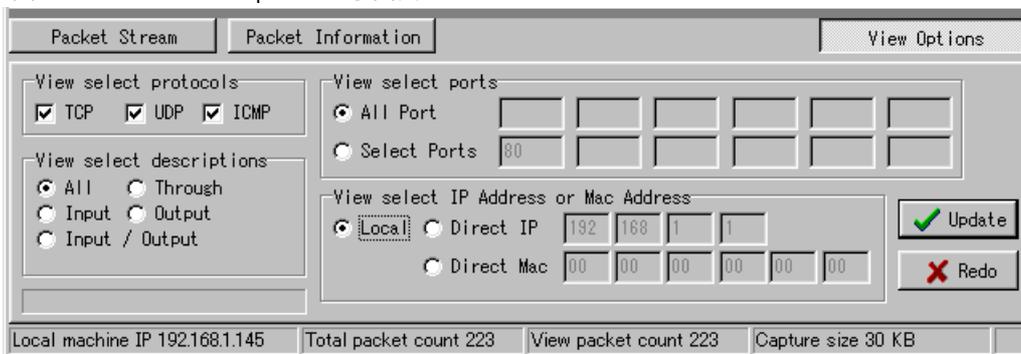


フィルタは以下の順で適用されます。

Capture select Protocols	キャプチャを行うプロトコルを選択します。
TCP	TCP(Transmission Control Protocol)有効/無効
UDP	UDP(User Datagram Protocol)有効/無効
ICMP	ICMP(Internet Control Message Protocol)有効/無効
Capture select Ports	キャプチャを行うポート番号を選択します。
All Ports	入力できる数値は10進数で0~65535までで12個まで設定できます。全てのポートを有効にします。
Select Ports	選択されたポートを有効にします。
Capture select IP address or MAC address	キャプチャの基準となるIPアドレス又はMACアドレスを設定します。この設定とDirection設定との組み合わせによりフィルタリング処理が行われます。
Local	ezMONITORを起動しているPCを基準とする
Direct IP	ここで設定されるIPアドレスを基準とする
Direct Mac	ここで設定されるMACアドレスを基準とする Windows2000では設定不可
Capture select Direction	パケットの流れる方向によるフィルタリングを行います。以下のどれか一つのみ選択でき、選択された条件のパケットが有効になります。
All	全てのパケット
Through	基準となるターゲット以外で送受信されているパケット
Input	基準となるターゲットに送信されたパケット
Output	基準となるターゲットから送信されたパケット
Input/Output	上記Input、Outputに該当するパケット
Capture Momory size	キャプチャデータを格納するために確保するメモリサイズを指定します。

2.2.2 表示用フィルタの設定 (Filter Option)

図 2.2 - 2 View Option 表示画面



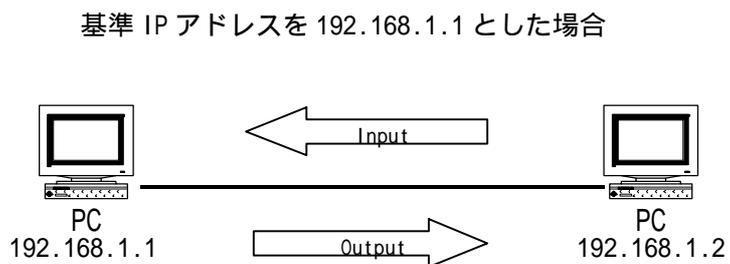
フィルタは以下の順で適用されます。

View select Protocols	表示を行うプロトコルを選択します。 TCP UDP ICMP	表示を行うプロトコルを選択します。 TCP(Transmission Control Protocol)有効/無効 UDP(User Datagram Protocol)有効/無効 ICMP(Internet Control Message Protocol)有効/無効
View select Ports	All Ports Select Ports	表示を行うポート番号を選択します。 入力できる数値は 10 進数で 0 ~ 65535 までで 1 2 個まで設定できます。 全てのポートを有効にします。 選択されたポートを有効にします。
View select IP address or MAC address	Local Direct IP Direct Mac	表示の基準となる IP アドレス又は MAC アドレスを設定します。この設定と Direction 設定との組み合わせによりフィルタリング処理が行われます。 EzMONITOR を起動している PC を基準とする ここで設定される IP アドレスを基準とする ここで設定される MAC アドレスを基準とする Windows2000 では設定不可
View select Direction	All Through Input Output Input/Output	パケットの流れる方向によるフィルタリングを行います。以下のどれか一つのみ選択でき、選択された条件のパケットが有効になります。 全てのパケット 基準となるターゲット以外で送受信されているパケット 基準となるターゲットに送信されたパケット 基準となるターゲットから送信されたパケット 上記 Input、Output に該当するパケット

### 2.2.3 Direction 指定の基準について

ezMONITOR は設定された IP アドレスもしくは MAC アドレスを基準にして Input/Output を定義します。  
また、Input/Output のどちらにも含まれないものを Through と定義します。

図 2.2-3 Direction の定義

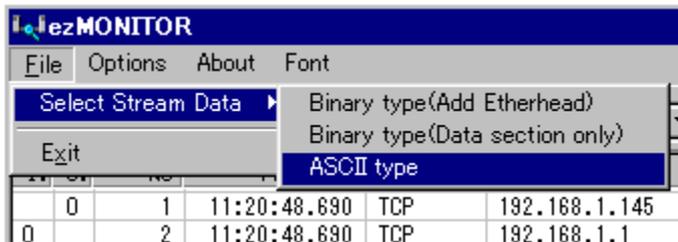


192.168.1.2(SourceIP)から 192.168.1.1(DestinationIP)へ送られるパケットは Input として分類され、  
192.168.1.1(SourceIP)から 192.168.1.2(DestinationIP)へ送られるパケットは Output として分類されます。

### 2.3 キャプチャデータ保存機能

ezMONITORはメモリ上にキャプチャしたデータをファイルとして保存しておくことができます。

図 2.3 - 1 キャプチャデータの保存



「File」 「Save Stream Data」を選択することによりファイルへの出力が可能です。  
 選択できるファイルフォーマットは以下の通りです。

Binary Type (Add etherhead)	キャプチャしたパケット全てをバイナリファイルとして保存
Binary Type (data section onry)	キャプチャしたパケットのデータ部分のみをバイナリファイルとして保存
ASCII type	キャプチャしたパケットをテキストファイルとして保存 パケットごとのテキストファイルのフォーマットは以下のようになります。

図 2.3 - 1 ASCII タイプでの保存形式

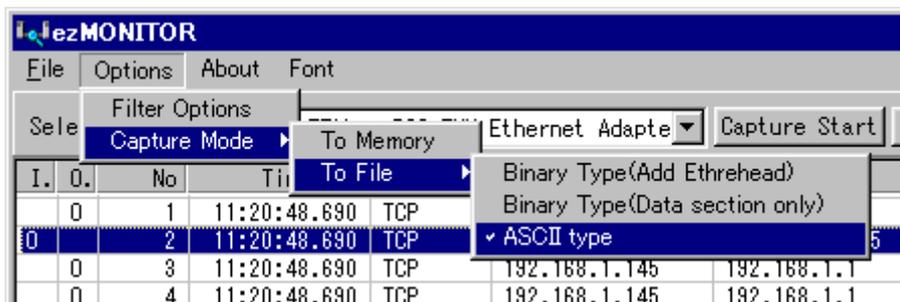
```

-----
00004
-----
[Time] 15:13:24.540
[Source Mac address] 00:90:99:22:F9:7F
[Destination Mac address] 00:00:E2:0D:37:42
[Ethernet type] 0800
[IP Version] 4
[Length] 254 byte
[Protocol] TCP
[Source IP] 192.168.1.145
[Destination IP] 192.168.1.1
[Source port] 1788
[Destination port] 10080
45 08 00 FE DC 2D 40 00 80 06 99 E1 C0 A8 01 91
C0 A8 01 01 06 FC 27 60 01 55 90 99 4A B7 1E A6
50 18 40 00 40 B9 00 00 47 45 54 20 68 74 74 70
3A 2F 2F 77 77 77 2E 61 70 6E 65 74 2E 63 6F 2E
6A 70 2F 20 48 54 54 50 2F 31 2E 30 0D 0A 41 63
63 65 70 74 3A 20 2A 2F 2A 0D 0A 41 63 63 65 70
74 2D 4C 61 6E 67 75 61 67 65 3A 20 6A 61 0D 0A
50 72 61 67 6D 61 3A 20 6E 6F 2D 63 61 63 68 65
0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F
7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 61
74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 35 3B
20 57 69 6E 64 6F 77 73 20 39 38 3B 20 54 33 31
32 34 36 31 29 0D 0A 48 6F 73 74 3A 20 77 77 77
2F 61 70 6F 65 74 2F 63 6F 2F 6A 70 0D 0A 50 72
    
```

## 2.4 ファイル出力機能

ezMONITORはキャプチャしたデータを逐次ファイルに記録する機能を持っています。  
この機能により、長時間で且つ大量のモニタ情報を保存することができます。

図 2.3 - 2 ファイル出力の設定



「Options」「Capture Mode」「To File」を選択することによりファイルへの出力モードになります。  
このモードを選択した場合、画面への出力はされずにパケットデータは直接ファイルに書き込まれることになります。

このモードは通常のモードと異なり、メモリの制限が無くなる為大量のパケットデータを記録できる利点があります。

## 2.5 メモリサイズについて

ezMONITORでキャプチャ可能なパケットの量は「Capture Option」の「Capture Memory Size」にて指定できます。  
設定可能なサイズは1~256MByteですが、大容量のメモリを確保してキャプチャを行う場合、正確にパケットを検出できない場合があります。

この原因は、パケット量の増大による ezMONITOR の処理速度の低下と OS により仮想メモリが使用されることによる PC パフォーマンスの低下が原因として上げられます。

これらについては ezMONITOR を実行する PC の能力や同時に実行しているその他のアプリケーションにより大きく左右される為、状況に応じて設定を変更する必要があります。

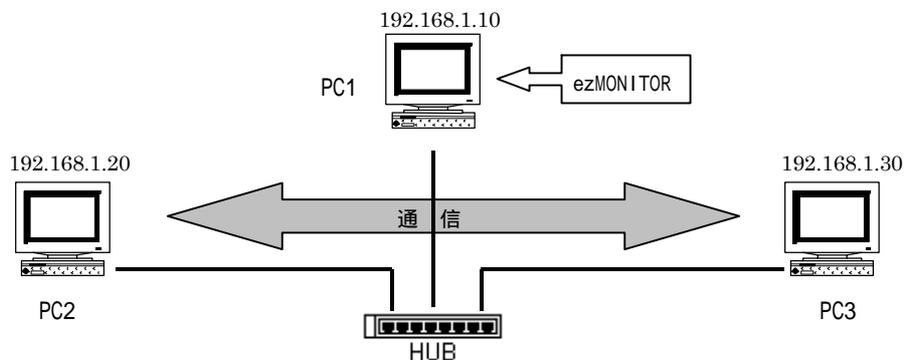
## 3. チュートリアル

本章では ezMONITOR を用いて実際にネットワーク上のパケットを取得する手順を説明します。

### 3.1 パケットのキャプチャ例

#### 3.1.1 他のネットワーク接続をモニタする

下記の図のように PC1 で ezMONITOR を起動し、PC2 PC3 の間に流れるパケットを監視します。  
 ここでの IP アドレスは PC1 を 192.168.1.10、PC2 を 192.168.1.20、PC3 を 192.168.1.30 としています。  
 これらの値はご使用の環境により変更してください。

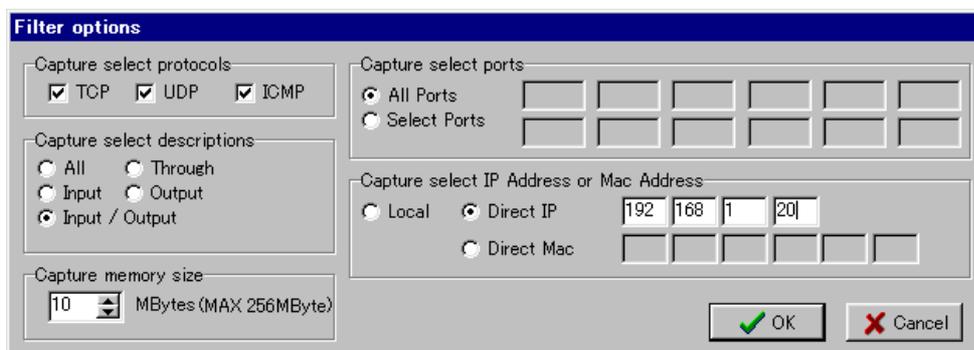


#### フィルタオプションの設定

ezMONITOR を起動し、「Options」 「Filter Options」を選択して、「Filter Options」を以下のように設定します。

Capture Select Protocols	全てチェック
Capture select Discriptions	「Input/OutPut」を選択
Capture select Ports	「All Ports」を選択
Capture Select IP Address or MAC Address	「Direct IP」 「192.168.1.20」を指定

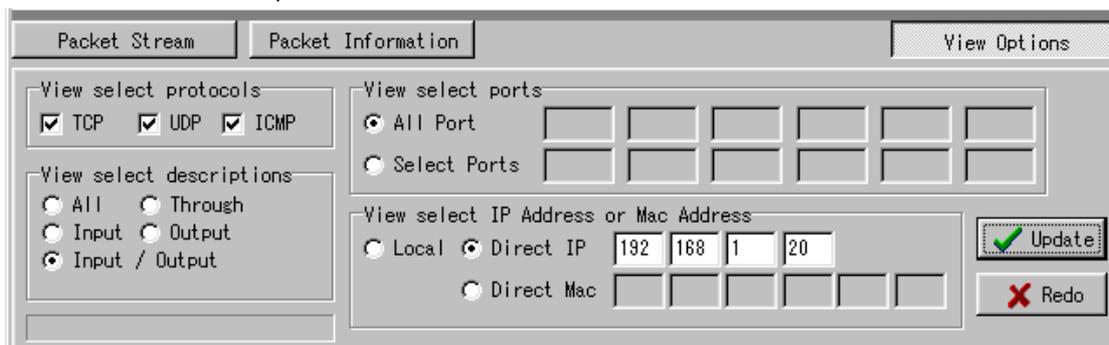
図 3.1-1 Filter Option の指定



同様に「View Options」を設定します。設定終了後に「Update」ボタンをクリックして設定を反映させてください。

View Select Protocols	全てチェック
View select Discriptions	「Input/output」を選択 (All でも同じです)
View select Ports	「All Ports」を選択
View Select IP Address or MAC Address	「Direct IP 」 「192.168.1.20」を指定

図 3.1 - 2 View Option の指定



#### ネットワークアダプタの選択

「Select Adapter」項目を LAN に接続されているネットワークアダプタに選択してください。

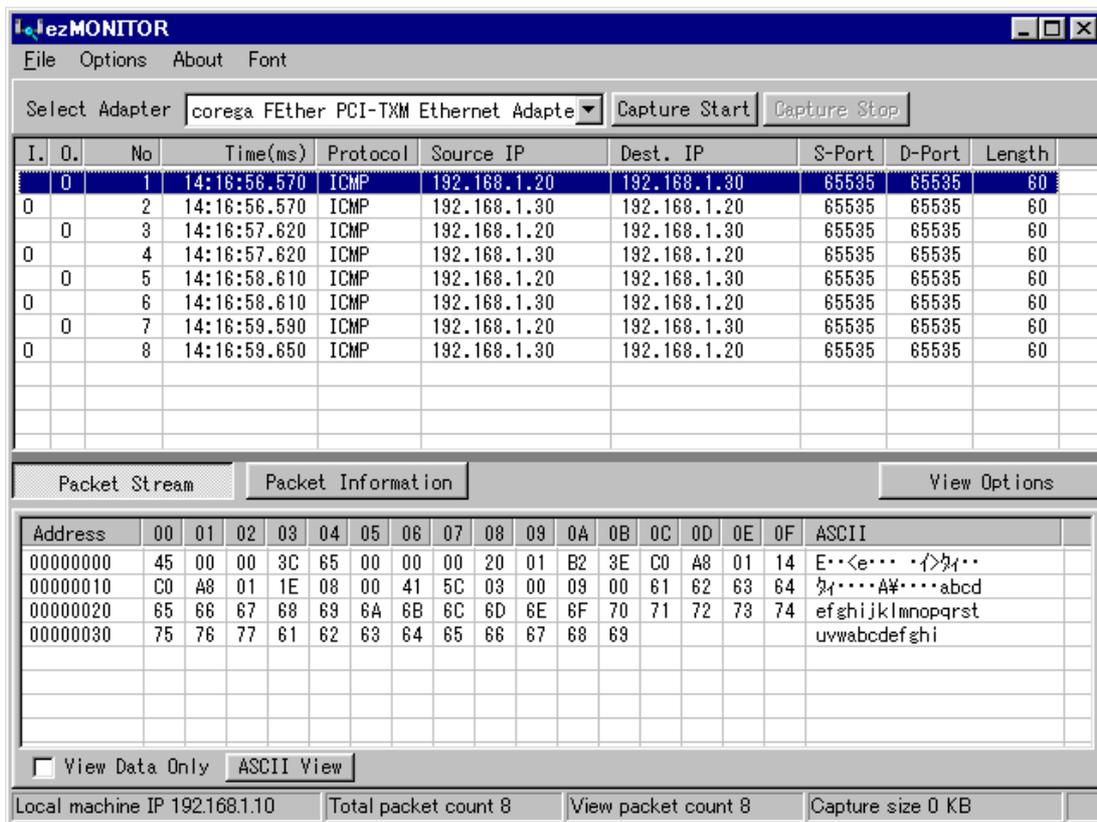
#### キャプチャの実行

「Capture Start」ボタンをクリックすることによりキャプチャが開始されます。

PC間の通信

試験的にPC間で通信を行ってみます。PC2上でWindowsの「スタート」 「ファイル名を指定して実行」で  
 "ping 192.168.1.30"と入力することによりPC2とPC3のパケット通信が行われます。(上記はDOSプロンプト  
 上でも同様のことが出来ます。)ezMONITOR上にパケットの情報が表示されていれば成功です。

図 3.1-3 Direct IP 指定でのモニタ結果

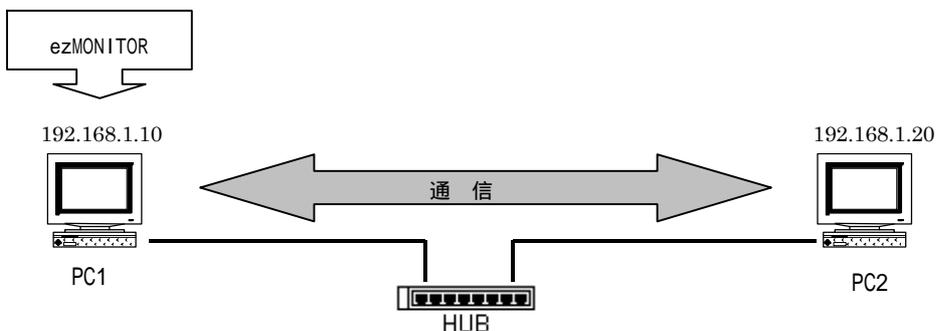


キャプチャの停止

「Capture Stop」ボタンをクリックすることによりキャプチャ動作を停止します。

### 3.1.2 自PCのネットワーク接続をモニタする

下記の図のようにPC1でezMONITORを起動し、PC1-PC2の間に流れるパケットを監視します。  
 ここでのIPアドレスはPC1を192.168.1.10、PC2を192.168.1.20としています。  
 これらの値はご使用の環境により変更してください。

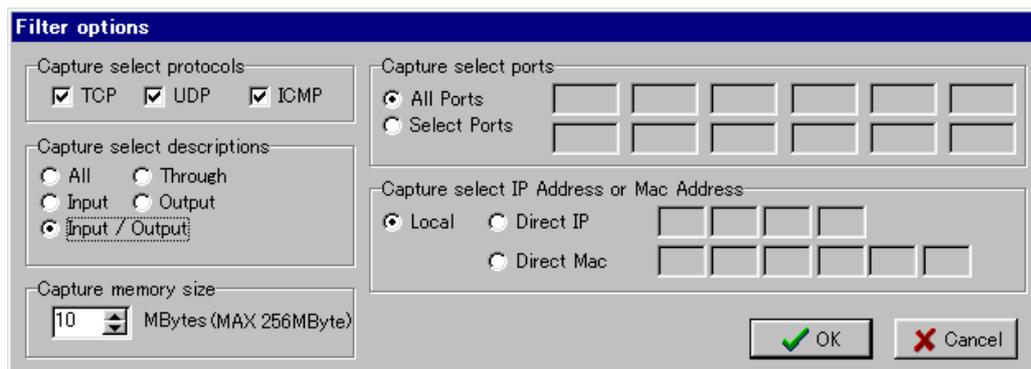


#### フィルタオプションの設定

ezMONITORを起動し、「Options」 「Filter Options」を選択して、「Filter Options」を以下のように設定します

- |  |                   |
|--|-------------------|
| Capture Select Protocols                 | 全てチェック            |
| Capture select Discriptions              | 「Input/OutPut」を選択 |
| Capture select Ports                     | 「All Ports」を選択    |
| Capture Select IP Address or MAC Address | 「Local」を指定        |

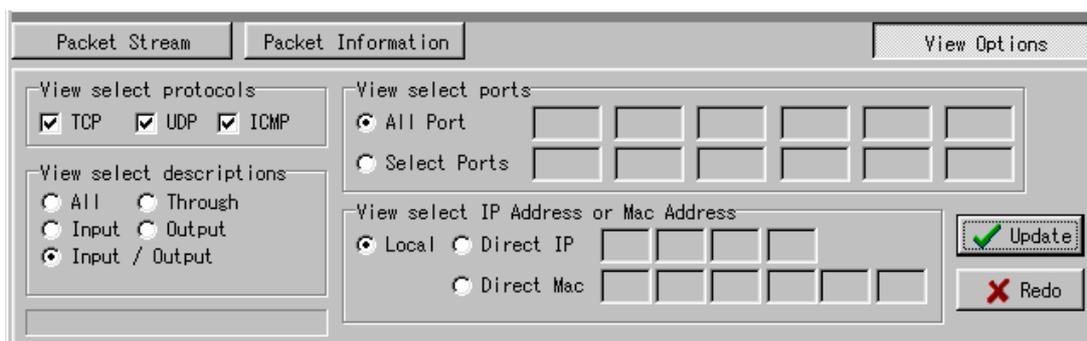
図 3.1-4 Filter Optionの指定



同様に「View Options」を設定します。設定終了後に「Update」ボタンをクリックして設定を反映させてください。

View Select Protocols	全てチェック
View select Discriptions	「Input/output」を選択 (All でも同じです)
View select Ports	「All Ports」を選択
View Select IP Address or MAC Address	「Local」を指定

図 3.1 - 5 View Option の指定



#### ネットワークアダプタの選択

「Select Adapter」項目を LAN に接続されているネットワークアダプタに選択してください。

#### キャプチャの実行

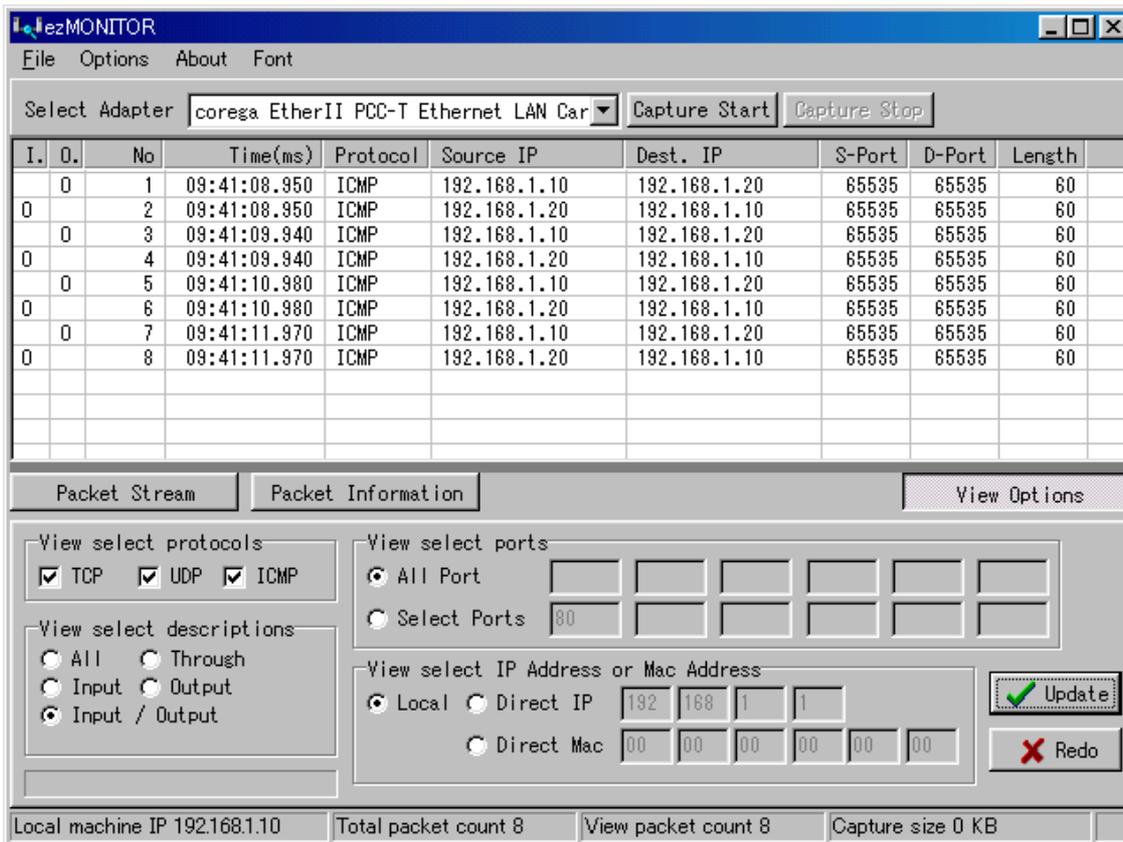
「Capture Start」ボタンをクリックすることによりキャプチャが開始されます。

PC間の通信

試験的にPC間で通信を行ってみます。PC1上でWindowsの「スタート」 「ファイル名を指定して実行」で  
 "ping 192.168.1.20" と入力することによりPC1とPC2のパケット通信が行われます。(上記はDOSプロンプト  
 上でも同様のことが出来ます。)

ezMONITOR 上にパケットの情報が表示されていれば成功です。

図 3.1-6 Local IP 指定でのモニタ結果



## 4 . トラブルシューティング

### 4 . 1 トラブルシューティング

- Q 1 . 「Capture Start」をクリックしてもパケットが表示されない。
- A 1 . 次のような原因が考えられます。
- 「Filter Option」の設定が正しくない 「Filter Option」を確認してください。
  - 「View Option」の設定が正しくない 「View Option」を確認してください。
  - 使用しているハブがスイッチングハブである スwitching機能の無いハブを使用してください。
  - ネットワークアダプタの選択が正しくない LANに接続されているネットワークアダプタを使用してください
- Q 2 . パケットデータを取りこぼす。
- A 2 . ezMONITORのキャプチャ能力はご使用のPCのパフォーマンスに大きく左右されます。キャプチャ中に他のアプリケーション等を動作させたりするとezMONITORの処理が遅れてしまい、パケットをキャプチャできない場合があります。また、キャプチャデータの総量が大きくなるとezMONITOR自体の処理が遅くなるため、パケットの取りこぼしが発生することがあります。そのような場合には、できるだけ高速なCPUと大容量のメモリを搭載したPCをお使いいただくことで改善されます。

## 5. 製品サポートと使用上の注意

### 5.1 製品サポートのご案内

#### 5.1.1 弊社ホームページのご利用について

弊社製品へのよくあるご質問及びご要望については、弊社ホームページ上のFAQに掲載しております。掲載内容につきましては随時更新されておりますので、是非ご利用ください。また、バージョンアップについてもホームページ上より提供しております。

弊社ホームページアドレス <http://www.apnet.co.jp/>

#### 5.1.2 製品サポートの方法

製品サポートについては、FAXもしくはE-MAILでのみ受け付けております。お電話でのお問い合わせは受け付けておりませんのでご了承ください。

##### 製品サポート窓口

FAXによるご連絡	053-464-3737
E-MAILによるご連絡	query@apnet.co.jp

お手数ですが、お問い合わせの際には、必ず製品のシリアル番号とお客様の会社名、お名前、ご連絡先(TEL,FAX,E-MAIL,etc)を明記してください。また、ご利用になっている環境を詳しく書き添えてください。

#### 5.1.3 製品サポートの範囲

以下の内容に該当するお問い合わせにつきましては、サポートの対象とはなりませんので、あらかじめご了承ください。

本製品のソフトウェア技術に関するご質問  
お客様が作成したアプリケーションプログラムに起因する問題やその解決方法についてのご相談  
一般的なネットワーク知識に関するご質問  
製品の仕様範囲外のご質問

### 5.2 使用上の注意

本製品を仕様範囲を越える条件において使用された場合、動作は保証しませんのでご了承ください。

本製品のリバースエンジニアリングは堅くお断りします。

宇宙、航空、医療、原子力、運輸、交通、各種安全装置など人命、事故に関わる特別な品質、信頼性が要求される用途でのご使用はご遠慮ください。

万が一、本製品を使用して事故または損失が発生した場合、弊社では一切の責を負いませんのでご了承ください。