ezTCP series

**TCP/IPネットワークプロトコルモニタ** 

## ezMONITOR

### 取り扱い説明書

第2版 2002/12/27

**ALPHA PROJECT CO.,LTD** 

### ezMONITOR 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 「ezMONITOR」 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 MONITOR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。

13

1

### 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	2	フィルタリング機能詳細		8
2.3	3	ファイル保存機能	1	1
2.4	4	ファイル出力機能	1	2
2.	5	メモリサイズについて	 1	2

### 3.チュートリアル

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

### 4 . トラブルシューティング 9

4.1 トラブル	シューティング		1	9
----------	---------	--	---	---

# 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</td> 20

J	•		表面 シハートの		2	U
5		2	使用上の注意		2	0

### 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。 e z MONITOR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

e z MONITOR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

e z MONITOR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	Windows95、98、Me、Windows2000が動作する
	PC/AT互換機
CPU	Pentium 300MHz以上
メモリサイズ	6 4 M B y t e 以上(1 2 8 M b y t e 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	Windows95、98、Me、Windows2000

Windows2000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。

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。

図1.3-1 ezMONITORの接続例

### 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

Leter Abort First															×
File Options About Font															
													2		
Select Adapte Corega	FEther	PCI-TX	M Ether	net /	Adap	te 💌	Ca	ptur	e St	art	Cap	ture Sto			
I.O. No Time	e(ms)	Protoco	I Sour	rce II	P		De	st.	IΡ			S-Port	D-Port	Length	
0 1 11:20:48	002	TCP	192	168.	1.14	5	19	2.16	8.1.	1		1038	10080	48	
0 2 11:20:48	8.690	TCP	192.	168.	1.1	-	19	2.16	8.1.	145		10080	1888	44	
0 3 11:20:48	8.690	TCP	192.	168.	1.14	5	19	2.16	8.1.	1		1038	10080	40	6
0 4 11:20:48	3.690	TCP	192	168.	1.14	5	19	2.16	8.1.	1		1038	10080	254	14
5 11:20:48	3.690	TCP	192.	168.	1.1		19	2.16	8.1.	145		10080	1038	171	-9
0 6 11:20:48	3.690	TCP	192.	168.	1.1		19	2.16	8.1.	145		10080	1038	1454	
0 7 11:20:48	3.800	TCP	192.	168.	1.14	5	19	2.16	8.1.	1		1038	10080	40	
8 11:20:48	3.800	TCP	192.	168.	1.1		19	2.16	8.1.	145		10080	1038	1454	
0 9 11:20:48	3.800	TCP	192.	168.	1.1		19	2.16	8.1.	145		10080	1038	1454	
0 10 11:20:48	3.960	TCP	192.	168.	1.14	5	19	2.16	8.1.	1		1038	10080	40	
0 11 11:20:48	3.960	TCP	192.	168.	1.1		19	2.16	8.1.	145		10080	1038	1454	
0 12 11•20•48	9 9 KH +	TOD	192	168	11		19	2 16	8 1	145	-	10080	1098	1454	
Packat Stream	Packet	Inform	ation	5								(	View	Options	10
	TACKET		acton	$\bigcirc$								1	TTC:	operions	-0
Address 00 01 02	03 0	)4 05	06 07	08	09	0A	0B	0C	0D	0E	0F	ASCII			١Ī
00000000 45 08 00	FF 4	¥E 00	40 00	80	06	07	0F	CO	A8	01	91	F••∎₀•®	· · · · · · · · · · · · · · · · · · ·		
00000010 C0 A8 01	01 0	14 OE	27 60	00	05	F1	85	4E	50	78	F9	5	••••••••••••••••••••••••••••••••••••••		
00000020 50 18 40	00 8	36 12	00 00	47	45	54	20	68	74	74	70	P-0	•GET http		
00000030 3A 2F 2F	77 7	77 77	2E 61	70	6E	65	74	2E	63	6F	2E	://www.	apnet.co.		
00000040 6A 70 2F	20 4	48 54	54 50	2F	31	2E	30	0D	0A	41	63	jp/ HTT	P/1.0.Ac	>	
00000050 63 65 70	74 3	3A 20	2A 2F	2A	0D	0A	41	63	63	65	70	cept: *	/*··Accep		
00000060 74 2D 4C	61 6	BE 67	75 61	67	65	3A	20	6A	61	0D	0A	t-Langu	age: ja•	•	
00000070 50 72 61	67 6	SD 61	3A 20	6E	6F	2D	63	61	63	68	65	Pragma:	no-cache	э	
└── View Data Only AS	CII Vie	ew													- <u>"</u>
ocal machine IP 192.168.1.1	45	Total pa	cket co	unt 22	23	Vie	w pa	cket	cour	nt 22	3	Capture	size 30 KE	3	

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。							
In	基準となるIPに対しての入力							
Out	基準となるIP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IPアドレス							
Dest. IP	送信先IP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ASCI
		I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

Packet S	et I	nfor	mati	on									View Options				
Address	00	01	02	03	04	05	06	07	08	09	0A	0B	00	0D	0E	0F	ASCII
00000000	45	08	00	FE	AA	2E	40	00	80	06	CB	E0	CO	A8	01	91	E・・■ェ.@・■・ビ络ィ・
00000010	C0	A8	01	01	07	14	27	60	01	77	6B	D7	4A	C6	D6	E1	ጶィ・・・・'`・wkラJ፲ヨ
00000020	50	18	40	00	AC	F6	00	00	47	45	54	20	68	74	74	70	P•®•∀ •GET http
00000030	3A	2F	2F	77	77	77	2E	61	70	6E	65	74	2E	63	6F	2E	://www.apnet.co.
00000040	6A	70	2F	20	48	54	54	50	2F	31	2E	30	0D	0A	41	63	јр/ НТТР/1.0••Ас 📃
00000050	63	65	70	74	3A	20	2A	2F	2A	0D	0A	41	63	63	65	70	cept: */*··Accep
00000060	74	2D	4C	61	6E	67	75	61	67	65	3A	20	6A	61	0D	0A	t-Language: ja••
00000070	50	72	61	67	6D	61	3A	20	6E	6F	2D	63	61	63	68	65	Pragma: no-cache
00000080	0D	0A	55	73	65	72	2D	41	67	65	6E	74	3A	20	4D	6F	••User-Agent: Mo
00000090	7A	69	60	8C	61	2F	34	2F	30	20	28	63	6F	6D	70	61	zilla/4.0 (compa 🛛 🔟
View Data Only ASCII View																	
Local machine	Local machine IP 192.168.1.145 Total packet cou									40	Vie	w pa	cket	cour	nt 140	)	Capture size 23 KB

### 図2.1-3 View Data Only 表示画面

Packet Stream Packet Information											View Options						
Address	00	01	02	03	04	05	06	07	08	09	0A	0B	00	OD	0E	0F	ASCII
00000000	47	45	54	20	68	74	74	70	3A	2F	2F	77	77	77	2E	61	GET http://www.a
00000010	70	6E	65	74	2E	63	6F	2E	6A	70	2F	20	48	54	54	50	pnet.co.jp/ HTTP
00000020	2F	31	2E	30	0D	0A	41	63	63	65	70	74	3A	20	2A	2F	/1.0…Accept: */
00000030	2A	0D	0A	41	63	63	65	70	74	2D	4C	61	6E	67	75	61	*••Accept-Langua
00000040	67	65	3A	20	6A	61	OD	0A	50	72	61	67	6D	61	3A	20	ge: ja••Pragma:
00000050	6E	6F	2D	63	61	63	68	65	0D	0A	55	73	65	72	2D	41	no-cache••User-A
00000060	67	65	6E	74	3A	20	4D	6F	7A	69	6C	6C	61	2F	34	2E	gent: Mozilla/4.
00000070	30	20	28	63	6F	6D	70	61	74	69	62	6C	65	3B	20	4D	0 (compatible; M 🔍
View Data Only ASCII View																	
ocal machine IP 192.168.1.145 Total packet co				t cou	int 20	70	Vie	w pa	cket	cour	nt 20	7	Capture size 29 KB				

#### 図2.1-4 ASCII View 表示画面



4

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

Packet Stream P	acket Information View Options				
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	5 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」ボタンで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	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
MAC address	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

Packet Stream Packet	Information	View Options
View select protocols TCP VIEW Select descriptions All C Through Input C Output Input / Output	View select ports C All Port Select Ports 80 View select IP Address or Mac Address C Local C Direct IP 192 168 1 1 C Direct Mac 00 00 00 00	Update Redo
Local machine IP 192.168.1.145	Total packet count 223 View packet count 223 Capture	size 30 KB

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

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	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
	or MAC address	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
```

Filter options	
Capture select protocols	Capture select ports C Select Ports C Select IP Address or Mac Address
<ul> <li>Input / Output</li> </ul>	€ Local C Direct IP     192     168     1     1
	C Direct Mac 00 00 00 00 00 00
Capture memory size	
MBytes (MAX 256MByte)	OK X Cancel

### 2.2 フィルタリング機能詳細

e z MONITOR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。 フィルター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 Fi	lter Options 表示画面
-----------	-------------------

Filter options	2
Capture select descriptions	
C Input C Output	Capture select IP Address or Mac Address
	C Direct Mac 00 00 00 00 00
Capture memory size	
	OK X Cancel

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。			
	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。			
All Ports	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	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			
MAC address	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。			
ALI	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
-----	-----	-----	------	--------	------

Packet Stream Packet Information	View Options
View select protocols View select ports View select descriptions All C Through C Input C Output C Input / Output C Input / Output C Direct Mac 00 00 00 00	DO Update Redo
Local machine IP 192.168.1.145 Total packet count 223 View packet count 223 Capture	size 30 KB

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	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			
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12個まで設定できます。			
All Ports	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。			
View select IP address or 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			
address	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			
View 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。			
ALI	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			

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

基準 IP アドレスを 192.168.1.1 とした場合



192.168.1.2(SourceIP)から 192.168.1.1(DestnationIP)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(DestnationIP) 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

e z MONITORはメモリ上にキャプチャしたデータをファイル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

lelez	MONITOR	۲.			
<u>F</u> ile	Options	About	Font		
Sel	ect Stream	Data 🛛	Binar	y type(	Add Etherhead)
<b>F</b> ::			Binar	y type(l	Data section only) 🛛 📙
	( 	<u> </u>	ASCI	l type	
	) 1	11:20	:48.690	TCP	192.168.1.145
0	2	11:20	:48.690	TCP	192.168.1.1

「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							
CO 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							
OD 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6E							
7A 69 6C 6C 61 2E 34 2E 30 20 28 63 6E 6D 70 61							
74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 35 3B							
20 57 69 6E 64 6E 77 73 20 39 38 3B 20 54 33 31							
32 34 36 31 29 0D 0A 48 6E 73 74 3A 20 77 77 77							
2F 61 70 6F 65 74 2F 63 6F 2F 64 70 0D 04 50 72							

### 2.4 ファイル出力機能

e z MONITOR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

ارا	ezN	IONITOF	<b>ર</b>			
<u>F</u> ile	• [	Options	About I	Font		
80		Filter O	ptions	<b></b>		China and Advanta W Conturn Start I
		Capture	: Mode 🕞	To M	lemory	Ethernet Adapte - Capture Start
Ι.	0.	No	Tiı	To F	ile 🔹 🕨	Binary Type(Add Ethrehead)
	0	1	11:20:4	48.690	TCP	Binary Type(Data section only)
0		2	11:20:4	18.690	TCP	✓ ASCII type
	0	3	11:20:4	48.690	TCP	192.168.1.145 192.168.1.1
	0	4	11:20:4	48.690	TCP	192.168.1.145 192.168.1.1

「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 P C 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に大きく左右 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			
Capture	select	Discriptions			
Capture	select	Ports			
Capture	Select	IP Address or MAC Address			

全てチェック 「Input/OutPut」を選択 「AII Ports」を選択 「Direct IP 」「192.168.1.20」を指定

#### 図 3.1-1 Filter Optionの指定

Filter options	
Capture select protocols	Capture select ports
C All C Through C Input C Output C Input / Output	Capture select IP Address or Mac Address C Local Direct IP 192 168 1 20
Capture memory size	C Direct Mac
10 MBytes (MAX 256MByte)	✓ OK X Cancel

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 (AII 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

Packet Stream Packet	Information	View Options
View select protocols TCP VIEW Select descriptions C All C Through C Input C Output View select descriptions	View select ports All Port Select Ports View select IP Address or Mac Address C Local © Direct IP 192 168 1 20	Update
	C Direct Mac	Redo

### 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。

### P C 間の通信

試験的に P C 間で通信を行ってみます。 P C 2 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 P C 2 と P C 3 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。

义	3.	. 1	- 3	Direct	IP 指定でのモニタ結果
---	----	-----	-----	--------	--------------

ارب	ezMONITOR																					
Eile Options About Font																						
Select Adapter Corega FEther PCI-TXM Ethernet Adapte 💌 Capture Start Capture Stop																						
Ι.	0.	No	)		Time	(ms)	Pr	otoc	ol	Sour	ce I	Р		De	st.	IP			S-Port	D-Port	Length	
	0			14:1	6:56	.570	IC	MP		192.	168.	1.20		19	2.16	8.1.	30		65535	65535	60	
0		2	2	14:1	6:56	.570	IC	MP		192.	168.	1.30		19	2.16	8.1.	20		65535	65535	60	
	0		}	14:1	6:57	.620	IC	MP		192.	168.	1.20		19	2.16	8.1.	30		65535	65535	60	
0	_	4	1	14:1	6:57	.620	IC	MP		192.	168.	1.30		19	2.16	8.1.	20		65535	65535	60	
_	0		5	14:1	6:58	.610	IC	MP		192.	168.	1.20		19	2.16	8.1.	30		65535	65535	60	
0	_	E	3	14:1	6:58	.610	IC	MP		192.	168.	$\frac{1.30}{1.30}$		19	2.16	8.1.	20		65535	65535	60	
	U		(	14:1	6:59	.590	IC	MP		192.	168.	1.20		19	2.16	8.1.	30		65535	65535	60	
U	0 8 14:16:59.650			IC	MP	_	192.168.1.30				192.168.1.20					65535	65535	60				
			-				-															
			-				-															
																						_
								U :	0-41													
	Pac	ket St	. rea	m		гаск	et I	ntor	mati	on										View	Uptions	
Ac	ldre:	25	00	01	02	03	04	05	06	07	08	09	ΠA	0B	00	ΠD	ΩE	0F	ASCLL			
0.0	0000	00	45	00	00	30	65	00	00	00	20	01	B2	3E	CO	A9	01	14	F/a	· ·/\b/·		
100	0000	10	C0	48	01	1F	0.0	00	41	50	03	00	02	00	61	62	63	64	LΔ	iz≱ ¥∙∙∙∙ahci	4	
00	0000	20	65	66	6 67 68 69 6A 6B			60	6D	6E	6F	70 71 72 73 74 efshiikimpoparst			ł							
00	00000030		75	76	77	61	62	63	64	65	66	67	68	69					uvwabcd	lefghi		
																				-		
Г	Vie	ew Dat	a Or	nly	ASC	CII V	iew															
Loca	al ma	achine	IP 1	92.16	8.1.1	0	То	ital p	acke	t cou	int 8		Vie	w pa	cket	cour	nt 8		Capture	size 0 KB		

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

### 図 3.1-4 Filter Optionの指定

Filter options								
Capture select protocols	Capture select ports C All Ports C Select Ports							
C All C Through	Capture select IP Address or Mac Address							
Input / Output	C Direct IP     C Direct IP     C  C     C							
	C Direct Mac							
Capture memory size								
10 🚔 MBytes (MAX 256MByte)	V OK K Cancel							

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 (AII 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

Packet Stream Packet	Information	View Options		
View select protocols TCP VIEW Select descriptions CALL C Through C Input C Output C Input / Output	View select ports  All Port  Select Ports  View select IP Address or Mac Address  Local C Direct IP  Direct Mac	Update Redo		

#### 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 P C 間で通信を行ってみます。 P C 1 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 P C 1 と P C 2 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

•	ez MC	DNITOR							<u>- 0 ×</u>		
<u>F</u> ile Options About Font			About Font								
Se	lect	Adapte	r corega Ether	II PCC-T E	thernet LAN Car 💌	Capture Start Capture Stop					
Ι.	0.	No	Time(ms)	Protocol	Source IP	Dest. IP	S-Port	D-Port	Length		
	0	1	09:41:08.950	ICMP	192.168.1.10	192.168.1.20	65535	65535	60		
0		2	09:41:08.950	ICMP	192.168.1.20	192.168.1.10	65535	65535	60		
	0	3	09:41:09.940	ICMP	192.168.1.10	192.168.1.20	65535	65535	60		
0		4	09:41:09.940	ICMP	192.168.1.20	192.168.1.10	65535	65535	60		
	0	5	09:41:10.980	ICMP	192.168.1.10	192.168.1.20	65535	65535	60		
0		6	09:41:10.980	ICMP	192.168.1.20	192.168.1.10	65535	65535	60		
	0	7	09:41:11.970	ICMP	192.168.1.10	192.168.1.20	65535	65535	60		
0		8	09:41:11.970	ICMP	192.168.1.20	192.168.1.10	65535	65535	60		
	Packet Stream     Packet Information     View Options										
View select descriptions         C All         C Input         Output         Input / Output         C Input / Output         O Input / Output         O Direct IP         1000000000000000000000000000000000000								Vupdate X Redo			
Loca	al ma	achine IP	192.168.1.10	Total pack	et count 8 View	v packet count 8	Capture	size 0 KB			

### 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

- Q1. 「Capture Start」をクリックしてもパケットが表示されない。
- A1. 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 スイッチング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。
- Q2. パケットデータを取りこぼす。
- A 2 . e z MONITOR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e z MONITOR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e z MONITOR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願います。 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。