

パケットキャプチャー機能(EEC) 操作マニュアル Ver2.0

EECにパケットキャプチャ機能を追加しました。

- ・ EECの試験自体をパケットキャプチャーすること
- ・ ミラーサイトを作り、パケットキャプチャーをすることが可能です。

起動、プロセスの中止、簡易検索がブラウザ上から行えます。

また、取得したパケットキャプチャーは、データをダウンロードして、WireSharkで検索することも可能です。

また、リモートEECとの情報共有機能を利用すれば、遠隔にあるEECのパケットキャプチャーの支持を行うことが可能です。

【改定履歴】

日付	内容	Ver
2017. 4. 6	初版	1.0
2018. 9. 3	突発トラヒック見える化,連続取得,複製	2.0

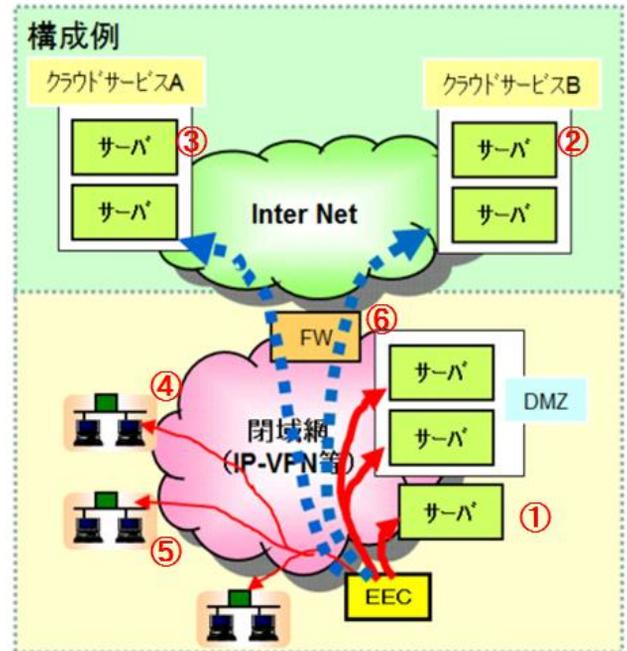
アイティエスコンサルティング株式会社
2018/9/3

1. システム
 - 1-1 EECの試験結果をパケットキャプチャーする場合の例
 - 1-2 ミラーポートを設置して、パケットキャプチャーを行う場合の例
2. 機能一覧
 - 2-1 起動
 - 2-2 検索1
 - 2-3 検索2
 - 2-4 その他
 - (1) プロセスの削除
 - (2) ログファイルの削除
 - (3) 上級者の起動
3. 突発トラヒック見える化
 - 3-1 突発トラヒック見える化の初期画面
 - 3-2 trapプログラムの起動画面
 - 3-3 trapプログラムの停止画面
4. 連続取得
 - 4-1 連続取得の初期画面
 - 4-2 連続取得の起動画面
 - 4-3 パケットデータの複製の初期画面
 - 4-4 複製の実行画面
 - 4-5 複製データの表示
 - 4-6 複製データの表示例

1. システム構成

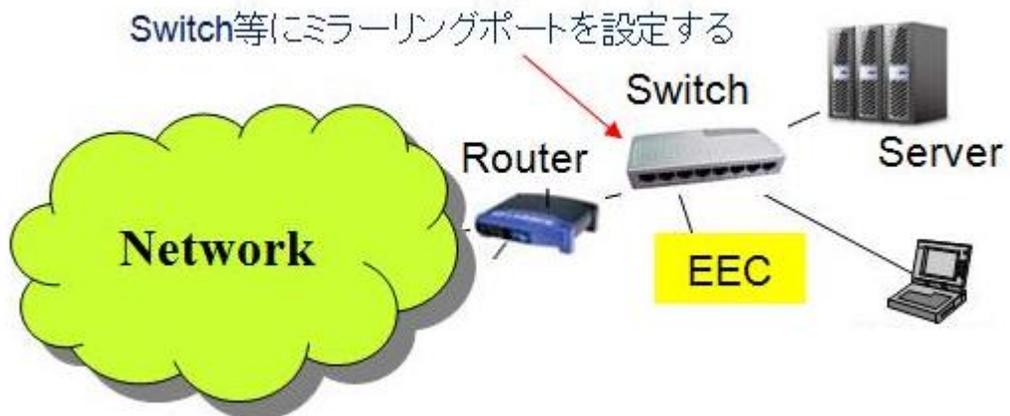
1-1 EECの試験結果をパケットキャプチャーする場合の例

右図のように、EECを設置し、その試験状況をパケットキャプチャーします。



1-2 ミラーポートを設置して、パケットキャプチャーを行う場合の例

パケットキャプチャーを行いたい箇所にミラーリングを行い、パケットキャプチャーを行います。



2-1 起動

Top画面 <http://ipアドレスorホスト名50ping/tcpdump/>

パケットキャプチャの起動

【検索1】

【検索2】

【起動】

Last Update:2016.10.21

レスポンスが遅くなった時、トラブルが発生した時に、本プログラムを起動して下さい。
指定したパケット数をキャプチャーをした後、自動で終了します。

(1) 抽出パケット数 万パケット

①

(2) パケットキャプチャーを行う機器のIPアドレス

指定しない場合は、全パケットになります。
指定したIPのみ抽出します。

②

(3) logのファイル名 ←半角英数字のみ “_”は使えます。

③

logファイルは、[指定した名前].cap, [指定した名前].cap1, [指定した名前].cap2, となります。

例：log_fileの場合 ⇒ log_file.cap, log_file.cap1, log_file.cap2, となります。 10Mbyte で分割します。

実行コマンド：

```
tcpdump -s0 -i eth0 -C 10 -Z root -c 指定したパケット数 -w 指定したファイル名.cap
```

ipアドレスが入力された場合

```
tcpdump -s0 -i eth0 -C 10 -Z root -c 指定したパケット数 -w 指定したファイル名.cap host 指定したIPアドレス
```

[上級者の起動のページへ](#)

現在起動中のtcpdumpプログラム [【プロセスの削除へ】](#) [【ログファイルの削除へ】](#)

起動中はありません

↑のプログラムが起動しています。追加で実行するが注意して下さい。

注意 パケットキャプチャーを行う機器にパケットが飛ばないアドレスを入れると、永遠に処理が続きます。

項目を選択します。

- ① : 取得するパケット個数を選択します。
- ② : オプション 取得したいIPを入力します。
- ③ : logのファイル名を入力します。

選択終了後、「起動」ボタンを押します。

2-1 起動 (つづき)

以下で、実行します。

- (1) 抽出パケット数: **0.1** 万パケット
- (2) パケットキャプチャーを行う機器のIPアドレス:
- (3) logのファイル名: **log_file**

【IPアドレスのチェック】
正しい IPアドレスです。(空欄も含まます)

【ファイル名のチェック】
正しいファイル名です。

【ファイル一覧】 赤字は、既にファイルが存在します。
03105M

実行コマンド: `tcpdump -s0 -i eth0 -C 10 -Z root -c 1000 -w /var/www/html/50ping/tcpdump/log_dir/log_file.cap`

内容をチェックして、正しいければ、「確定」ボタンを押します。パケットキャプチャーが始まります。

実行しました。

加算が長いとブラウザが止まります。

[起動処理のトップ画面に移動](#)して下さい。

【注意】 リーロードはしないで下さい。

同じプログラムが同時に走ってしまいます。
上のリンクの、「起動処理のトップ画面に移動」を利用してください。

実行コマンド

`tcpdump -s0 -i eth0 -C 10 -Z root -c 1000 -w /var/www/html/50ping/tcpdump/log_dir/log_file.cap`

◆赤字の【終了しました】が出るまで、このままにするか、トップ画面に移動して下さい。
画面を開いてもプログラムは継続します。

パケットキャプチャーが開始されました。
「起動処理のトップ画面に移動」をクリックして下さい。

【補足】

パケットキャプチャは、10Mbyte毎にファイルが分割されます。

パケットキャプチャの検索 (その1)

【検索1】

【検索2】

【起動】

【logファイル一覧】

z_6000.cap log fileを選択 または log file名を直接入力して下さい。
 直接入力の方が優先されます。

①

【Jobを選択して下さい】 IP 名前に変換

（事前に、名前がダイナミックに変わることがあります。その場合は IP を選択して下さい。）

②

J1-1 パターン検索 番目から表示

検索したい文字を入力して下さい。例: http, smtp, 192.168.70 等 and 検索

③

←その1 含む 含まない

←その2 含む 含まない

←その3 含む 含まない

↑その1から入力して下さい。入力しなくても構いません。

J1-2 ひと塊り処理の検索 (処理毎に変わるポート番号をを入力)

↑ポート番号の入力。例: watt.sys.net.55367 の 55367等

④

を超えると赤色で出力

④

注意: 名前の場合、処理時間がかかることがあります。その際は、IPをご利用下さい。

検索の実行 クリア

項目を選択します。

① logファイル名をリストから選択するか、直接logファイル名を入力します。

② J1-1 パターン検索

or

J1-2 ひと塊り処理の検索 を選択します。

③は、J1-1を選択した時に有効です。

④は、J1-2を選択した時に有効です。

J1-1 パターン検索 の実行例

パケットキャプチャ-の検索結果のページ

logファイル名 : **log_file.cap** [ipで表示]検索結果 検索キー(1) : **http** (含む) 検索キー(2) : **[S]** (含む) 検索キー(3) : 1 番目から表示

```

1 32 16:03:01.248414 IP 133.242.130.174.37748 > 119.245.180.154.http: Flags [S], seq 407297615, win 14600, options
2 146 16:03:02.272744 IP 133.242.130.174.60423 > 202.232.88.94.http: Flags [S], seq 1260396552, win 14600, options
3 195 16:03:03.310362 IP 133.242.130.174.37748 > 202.232.88.91.http: Flags [S], seq 3901515979, win 14600, options
4 243 16:03:04.358755 IP 133.242.130.174.51630 > 202.232.88.92.http: Flags [S], seq 4009502648, win 14600, options
5 321 16:03:05.347233 IP 153.149.167.67.38136 > 133.242.130.174.http: Flags [S], seq 571673420, win 14600, options
6 344 16:03:05.448594 IP 133.242.130.174.41571 > 203.216.198.168.http: Flags [S], seq 4200635582, win 14600, optior
7 412 16:03:06.471661 IP6 2401:2500:102:1102:133:242:130:174.33446 > 2404:6800:4004:81a::2003.http: Flags [S], seq
8 806 16:03:07.494656 IP 133.242.130.174.54070 > 182.50.78.61.http: Flags [S], seq 4088481200, win 14600, options
9 856 16:03:07.699797 IP 61.213.120.187.58628 > 133.242.130.174.http: Flags [S], seq 1432826747, win 14600, options

```

次のページ

TOPへ

[検索のTOPページへ](#)

ひとつ前に戻る

J1-2 ひと塊り処理の検索 の実行例

上の赤枠の 37748 ポートを指定場合

パケットキャプチャ-の検索結果のページ

logファイル名 : **log_file.cap** [ipで表示]検索結果 ポート番号 : **37748** task_time : **200** ms [ひとつ前に戻る](#)

No	Time	task time	IP	Sorce Dept	Dest Dept	Flag	Ack	Length
1	16:03:01.248414		IP	133.242.130.174.37748	119.245.180.154.http	[S]		length 0
2	16:03:01.267533	0.019119	IP	119.245.180.154.http	133.242.130.174.37748	[S.]	[ACK]	length 0
3	16:03:01.267605	0.000072	IP	133.242.130.174.37748	119.245.180.154.http	[.]	[ACK]	length 0
4	16:03:01.267712	0.000107	IP	133.242.130.174.37748	119.245.180.154.http	[F.]	[ACK]	length 0
5	16:03:01.286908	0.019196	IP	119.245.180.154.http	133.242.130.174.37748	[.]	[ACK]	length 0
6	16:03:01.291212	0.004304	IP	119.245.180.154.http	133.242.130.174.37748	[F.]	[ACK]	length 0
7	16:03:01.291241	0.000029	IP	133.242.130.174.37748	119.245.180.154.http	[.]	[ACK]	length 0

パケットキャプチャの検索 (その2)

【検索1】

【検索2】

【起動】

【logファイル一覧】

z_6000.cap

←log fileを選択 または、log_file.cap

log file名を直接入力して下さい。

↑ 直接入力の方が優先されます。

【Jobを選択して下さい】

 IP 名前に変換←J2-3のみ)

(※4桁に、名前がランダムに変わる場合があります。その時はIPを選択して下さい。)

 J2-1 IPレイヤの分類 J2-2 IPプロトコル種別の一覧(Top 20) J2-3 IPアドレス(Top 10)

【送信元】及び【送信先】

<出力例>

```
ARP : 4613
IP : 1066
IP6 : 321
```

【送信元】

```
1 .domain 2438
2 .http 1043
3 .https 535
```

【送信先】

```
1 .domain: 2503
2 .http: 1288
3 .https: 625
```

<出力例>

```
【送信元】
1 watt-sys.net 5168
2 j120187.ppp.asahi-net.or.jp 542
3 ns1.dns.ne.jp 480
4 bigpark.org 314
```

【送信先】

```
1 watt-sys.net 4812
2 j120187.ppp.asahi-net.or.jp 483
3 ns1.dns.ne.jp 480
```

注意: J2-2, J2-3 は、ICPM, Advertisement, ARP, IP6, fe80::1(IP6関連) を除いています。
名前の場合、処理時間がかわかることがあります。その際は、IPをご利用下さい。

検索の実行

クリア

J2-1 IPレイヤの分類 の実行例

パケットキャプチャの検索結果のページ

【logファイル名 (識別子)】 : log_file.cap

IPレイヤの分類 (パケット数)

ひとつ前に戻る

```
ARP : 733
IP : 253
IP6 : 14
```

J2-2 IPプロトコル種別の一覧 の実行例

パケットキャプチャの検索結果のページ

【logファイル名 (識別子)】 : log_file.cap

IPプロトコルのポート種別の一覧

ひとつ前に戻る

【送信元】

```
1 .domain 58
2 .smtp 27
3 .http 24
4 .flashfiler 5
5 .imaps 3
6
```

J2-3 IPアドレス の実行例

パケットキャプチャの検索結果のページ

【logファイル名 (識別子)】 : log_file.cap

IPアドレス(Top30)

ひとつ前に戻る

【送信元】

```
1 133.242.130.174 124
2 202.238.84.12 15
3 202.238.84.192 11
4 68.59.87.23 10
5 75.74.13.66 8
```

パケットキャプチャの起動

【検索1】

【検索2】

【起動】

Last Update: 2016.10.21

レスポンスが遅くなった時、トラブルが発生した時に、本プログラムを起動して下さい。
指定したパケット数をキャプチャーをした後、自動で終了します。

(1) 抽出パケット数 万パケット

(2) パケットキャプチャーを行う機器のIPアドレス

指定しない場合は、全パケットになります。

指定したIPのみ抽出します。

(3) logのファイル名 ←半角英数字のみ “_”は使えます。

logファイルは、[指定した名前].cap, [指定した名前].cap1, [指定した名前].cap2, となります。

例：log_fileの場合 ⇒ log_file.cap, log_file.cap1, log_file.cap2, となります。 10Mbyte で分割します。

実行コマンド：

tcpdump -s0 -i eth0 -C 10 -Z root -c 指定したパケット数 -w 指定したファイル名.cap

ipアドレスが入力された場合

tcpdump -s0 -i eth0 -C 10 -Z root -c 指定したパケット数 -w 指定したファイル名.cap host 指定したIPアドレス

起動 クリア

[上級者の起動のページへ](#)

①

③

現在起動中のtcpdumpプログラム

[【プロセスの削除へ】](#)

[【ログファイルの削除へ】](#)

②

起動中にはありません

↑のプログラムが起動しています。追加で実行するが注意して下さい。

注意 パケットキャプチャーを行う機器にパケットが飛ばないアドレスを入れると、永遠に処理が続きます。

トップ画面のページより、リンクがあります。

- ① (1) プロセスの削除
- ② (2) ログファイルの削除
- ③ (3) 上級者の起動

リンク先のガイダンスに従い実行して下さい。

3-1 突発トラヒック見える化の初期画面

http://www.glcom.co.jp/itsr/burst_traffic.html を参照願います。↓ クリックします

パケットキャプチャーの起動

[検索1] [検索2] [起動] [マニュアル] [高度統計] **[突発traffic]** [連続取得]

レスポンスが遅くなった時、トラブルが発生した時に、本プログラムを起動して下さい。
指定したパケット数をキャプチャーをした後、自動で終了します。

(1) 抽出パケット数 万パケット

(2) パケットキャプチャーを行う機器のIPアドレス

指定しない場合は、全パケットになります。

指定したIPのみ抽出します。

3-2 trapプログラムの起動画面

突発トラヒック見える化 trap プログラムの起動

[パケットキャプチャTOP] [Trapプログラムの停止]

アラームを検知すると自動でパケットキャプチャーが起動します。本Trapプログラムは、終了します。
本trapプログラムは、1回のみパケットキャプチャーを起動します。もう1度パケットキャプチャーを行う場合は、

(A) センタEECのIPアドレス

①

←トリガのAlarmを入手するEECを指定します。
自分自身のEECでも構いません。

(B) 識別名：alarm_now に表示される項目の一覧となる識別項目

IPアドレス や 検出名... 等の項目 例：10.1.20.35 or tokubetsu_kansi_3 等

(1) 抽出パケット数 万パケット

②

←抽出するパケット数を指定します。

(2) パケットキャプチャーを行う機器のIPアドレス

指定しない場合は、全パケットになります。

指定したIPのみ抽出します。

③

←IPを絞り込み時に指定します。

④

←File名を指定します。

(3) logのファイル名

←半角英数字のみ "_" は使えます。

logファイルは、[指定した名前_プロセス番号].cap , [指定した名前_プロセス番号].cap1, [指定した名前_プロセス番号].cap2,
例：log_fileの場合 ⇒ log_file_1234.cap, log_file_1234.cap1, log_file_1234.cap2, となります。 10Mbyte で分割します
実行コマンド：

tcpdump -s0 -i eth0 -C 10 -Z root -c 指定したパケット数 -w 指定したファイル名_プロセス番号.cap

ipアドレスが入力された場合

tcpdump -s0 -i eth0 -C 10 -Z root -c 指定したパケット数 -w 指定したファイル名_プロセス番号.cap host 指定したIP

⑤

←起動ボタンを押すと、トラッププログラムが起動します。
アラートが発生するまで、パケットキャプチャーは実行されません。

3-3 trapプログラムの停止画面

起動中の時クリックをします

突発トラヒック見える化 trap プログラムの起動 [\[パケットキャプチャTOP\]](#) [\[Trapプログラムの停止\]](#) **起動中**

アラームを検知すると自動でパケットキャプチャーが起動します。本Trapプログラムは、終了します。
本trapプログラムは、1回のみパケットキャプチャーを起動します。もう1度パケットキャプチャーを行う場合は、本プロ

(A) センタEECのIPアドレス

16(.....)

(B) 識別名：alarm_now に表示される項目の一意となる識別項目

10.1.16.11

3-4 trapプログラムの停止

突発トラヒック tcpdump トラッププログラムの削除

[ひとつ前に戻る](#)

現在起動中のトラッププログラムのプロセス [削除するプロセスを選んで下さい。](#)

5 14 ? S 0:00 /usr/bin/perl /var/www/cgi-bin/50ping/tcpdump/t_traffic_tcpdump_trap_kido.pl 16..... 10.1.16.11

[確認のページへ](#)

[クリア](#)

プロセスを選択し、確認のページへ のボタンを押して下さい。

後は、ガイダンスに従い、trap プログラムの停止を行って下さい。

4 連続取得

4-1 連続取得の初期画面

クリックをします ↓

パケットキャプチャ-の起動

[検索1] [検索2] [起動] [マニュアル] [高度統計] [突発traffic] 連続取得

レスポンスが遅くなった時、トラブルが発生した時に、本プログラムを起動して下さい。
指定したパケット数をキャプチャーをした後、自動で終了します。

(1) 抽出パケット数 万パケット

(2) パケットキャプチャーを行う機器のIPアドレス

指定しない場合は、全パケットになります。

4-2 連続取得の起動画面

連続取得プログラムの起動

[パケットキャプチャTOP] [連続取得プログラムの停止] 停止中 [Snap_Shot]

パケットキャプチャーを連続して行います。指定した取得パケット数を過去5世代蓄積します。
過去五世代を蓄積していますので、トラブル（遅延等）が生じる前からの状況を把握する時に便利です。
トラブル（遅延等）があった場合は、本プログラムを停止して、パケット連続取得を停止して下さい。停止
ピーを取り保存して下さい）。

(1) 抽出パケット数 万パケット **①** ←抽出するパケット数を指定します。

(2) パケットキャプチャーを行う機器のIPアドレス

<input type="text"/>

指定しない場合は、全パケットになります。

指定したIPのみ抽出します。

② ←IPを絞り込み時に指定します。

(3) logのファイル名は、固定されています。

renzoku_0.capです。renzoku_0.cap1, renzoku_0.cap2, ... 1ファイルは10Mbyteに分割されています。

過去の世代は、新しいものから、renzoku_1.cap, renzoku_1.cap1, renzoku_1.cap2, ...

renzoku_2.cap, renzoku_2.cap1, renzoku_2.cap2, ...

renzoku_3.cap, renzoku_3.cap1, renzoku_3.cap2, ...

renzoku_4.cap, renzoku_4.cap1, renzoku_4.cap2, ...

renzoku_5.cap, renzoku_5.cap1, renzoku_5.cap2, ...となります。

実行コマンド:

tcpdump -s0 -i eth0 -C 10 -Z root -c 指定したパケット数 -w renzoku_0.cap

ipアドレスが入力された場合

tcpdump -s0 -i eth0 -C 10 -Z root -c 指定したパケット数 -w renzoku_0.cap host 指定したIPアドレス

③

↑ 起動ボタンを押して、確認画面に進んで下さい。
後は、ガイダンスに従い、起動を行って下さい。

4-3 パケットデータの複製の初期画面

Snap Shotをクリックをします ↓

連続取得プログラムの起動

[パケットキャプチャTOP] [連続取得プログラムの停止] 停止中

Snap Shot

パケットキャプチャーを連続して行います。指定した取得パケット数を過去5世代蓄積します。過去五世代を蓄積していますので、トラブル（遅延等）が生じる前からの状況を把握する時に便利です。トラブル（遅延等）があった場合は、本プログラムを停止して、パケット連続取得を停止して下さい。停止ピーを取り保存して下さい。

(1) 抽出パケット数 万パケット

(2) パケットキャプチャーを行う機器のIPアドレス

指定しない場合は 全パケットになります

4-4 複製の実行画面

連続取得パケットデータの複製

ひとつ前に戻る

[現状の複製データ状況]

現在連続パケットデータの取得状況 ファイルは刻々と変わっています。連続取得プログラムが動作中の時は、データの不整合がある
renzoku_0.cap

```
-rw-r--r-- 1 root root 10000028 Aug 30 18:20 /var/www/html/50ping/tcpdump/log_dir/renzoku_0.cap
~
```

```
-rw-r--r-- 1 root root 2616650 Aug 30 18:20 /var/www/html/50ping/tcpdump/log_dir/renzoku_0.cap1
renzoku_1.cap
```

```
-rw-r--r-- 1 root root 10011948 Aug 30 18:18 /var/www/html/50ping/tcpdump/log_dir/renzoku_1.cap
~
```

```
-rw-r--r-- 1 root root 4165828 Aug 30 18:18 /var/www/html/50ping/tcpdump/log_dir/renzoku_1.cap1
renzoku_2.cap
```

```
-rw-r--r-- 1 root root 10003835 Aug 30 18:18 /var/www/html/50ping/tcpdump/log_dir/renzoku_2.cap
~
```

```
-rw-r--r-- 1 root root 3213474 Aug 30 18:18 /var/www/html/50ping/tcpdump/log_dir/renzoku_2.cap1
renzoku_3.cap
```

```
-rw-r--r-- 1 root root 10003259 Aug 30 18:17 /var/www/html/50ping/tcpdump/log_dir/renzoku_3.cap
~
```

```
-rw-r--r-- 1 root root 3425948 Aug 30 18:17 /var/www/html/50ping/tcpdump/log_dir/renzoku_3.cap1
renzoku_4.cap
```

```
-rw-r--r-- 1 root root 10010815 Aug 30 18:16 /var/www/html/50ping/tcpdump/log_dir/renzoku_4.cap
~
```

```
-rw-r--r-- 1 root root 3344086 Aug 30 18:16 /var/www/html/50ping/tcpdump/log_dir/renzoku_4.cap1
renzoku_5.cap
```

```
-rw-r--r-- 1 root root 10009315 Aug 30 18:16 /var/www/html/50ping/tcpdump/log_dir/renzoku_5.cap
~
```

```
-rw-r--r-- 1 root root 5072124 Aug 30 18:16 /var/www/html/50ping/tcpdump/log_dir/renzoku_5.cap1
```

最終確認ボタン

クリア

←複製を作成します。

↑ 最終確認ボタンを押すと、現時点のデータ、過去5世代のデータを複製します。

4 連続取得

4-5 複製データの表示

クリックをします ↓

連続取得パケットデータの複製

[ひとつ前に戻る](#)[\[現状の複製データ状況\]](#)[\[連続取得_top\]](#)

次の複製を行いました。 /var/www/html/50ping/tcpdump/log_dir/bk/ 配下に保存されます。

例：renzoku_0_180901_154605.cap

renzoku_0.cap

cp /var/www/html/50ping/tcpdump/log_dir/renzoku_0.cap /var/www/html/50ping/tcpdump/log_dir/bk,
~

cp /var/www/html/50ping/tcpdump/log_dir/renzoku_0.cap1 /var/www/html/50ping/tcpdump/log_dir/bl
renzoku_1.cap

cp /var/www/html/50ping/tcpdump/log_dir/renzoku_1.cap /var/www/html/50ping/tcpdump/log_dir/bk,
~

cp /var/www/html/50ping/tcpdump/log_dir/renzoku_1.cap1 /var/www/html/50ping/tcpdump/log_dir/bl

4-6 複製データの表示例

現状の複製データ状況

[ひとつ前に戻る](#)[\[連続取得_top\]](#)

/var/www/html/50ping/tcpdump/log_dir/bk/ 配下の情報

cap群	総file数	削除
renzoku_0_180901_163133.cap	20	<input type="checkbox"/>
renzoku_0_180901_165302.cap	6	<input type="checkbox"/>
renzoku_0_180902_134901.cap	6	<input type="checkbox"/>
renzoku_0_180903_092807.cap	6	<input type="checkbox"/>

[削除](#)[クリア](#)

ディスク容量

```
Filesystem      1K-blocks      Used Available Use% Mounted on
/dev/vda3       100893076 44854988 50912920 47% /
tmpfs           510108         0      510108  0% /dev/shm
/dev/vda1       247919         53696  181423  23% /boot
```

この画面から、複製データの削除が行えます。
削除したい cap群を指定し、削除ボタンを押して下さい。
その後は、ガイダンスに従って下さい。