パケットキャプチャー機能（EEC）
操作マニュアル_検索３ v1.1

EECにパケットキャプチャーの検索機能を大幅に改善をしました。
・リアルタイム系検索の充実
・snap shot （データのコピー）で取得したデータの検索機能の充実

この機能により、お客様自身による、一般的なパケットキャプチャーの分析が可能となりました。

問題発生時の即座の検索により、原因の発見の強力な支援ツールとなります。

本機能以外については、『パケットキャプチャ操作マニュアルv2』をご参照下さい。

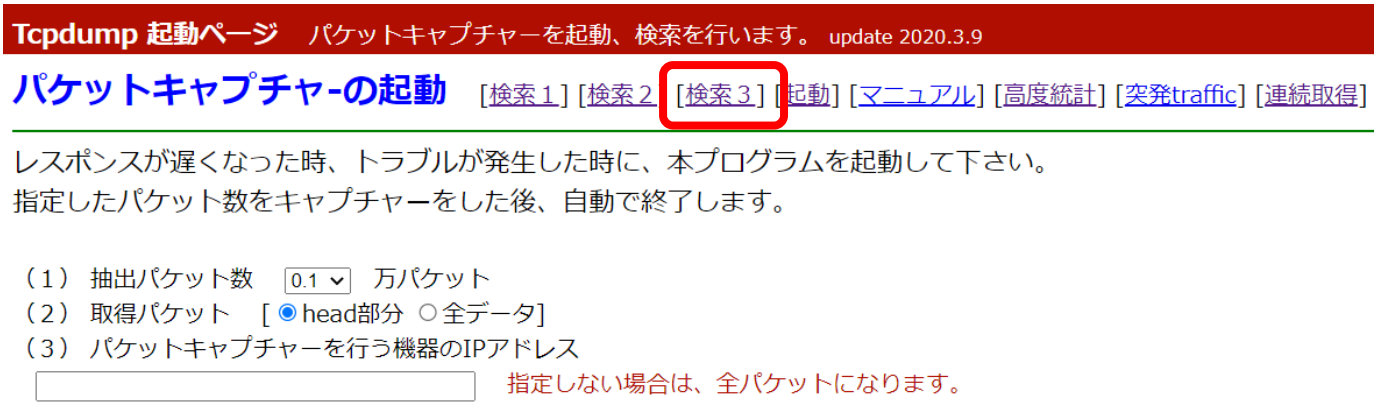
【改定履歴】

日付	内容	Ver
2023. 1. 18	初版	1.0
2023. 2. 5	リアルタイムの説明を追加、棒グラフ表示追加	1.1

アイティエスコンサルティング株式会社
2023/2/5

目次

お客様のお手元のPCより、
http://EECのIPアドレス/50ping/tcpdump/　にて
パケットキャプチャーの　TOP画面を開きます。

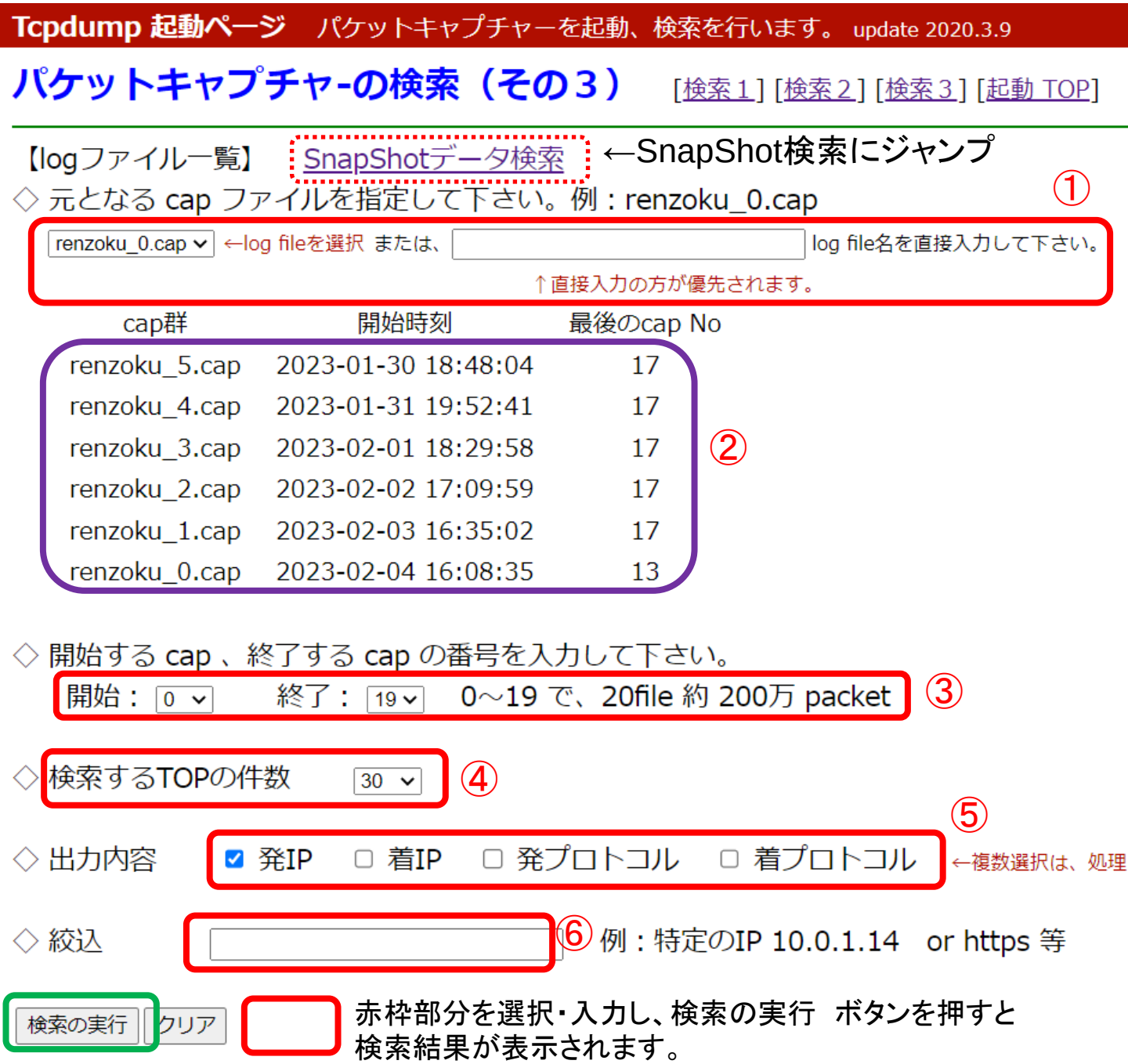


[検索3]　をクリックします。

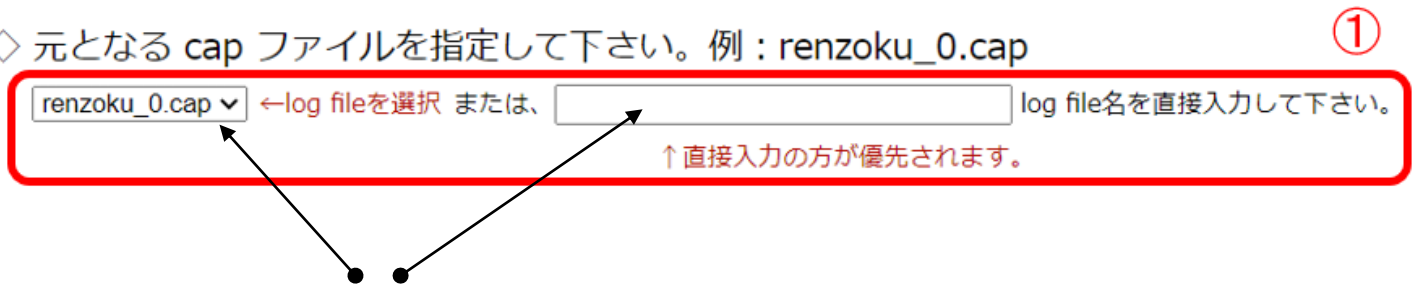
すると　検索3　の　TOP　画面のページに移ります。

次ページに示します。

リアルタイム系の検索



①～⑥ について、詳細を次ページ以降で説明します。



左の pull downメニューで選択するか、
または、右側の box に直接入力して下さい。

cap群	開始時刻	最後のcap No
renzoku_5.cap	2023-01-30 18:48:04	17
renzoku_4.cap	2023-01-31 19:52:41	17
renzoku_3.cap	2023-02-01 18:29:58	17
renzoku_2.cap	2023-02-02 17:09:59	17
renzoku_1.cap	2023-02-03 16:35:02	17
renzoku_0.cap	2023-02-04 16:08:35	13

②

5世代の最初のファイル cap の 開始時刻　及び　最後のcap No を示します。

この例では、1世代が200万パケットとしていますので、
cap のファイル数は、約 20 file（実際は、0～17 の 18file ）となっています。
600万世代の場合は、58file 程度になります。
renzoku_0 群は、今、まさにキャプチャーをしている世代です。
cap No が　**13** となっていますので、現在　約 140万 packet のキャプチャーデータがあることが分かります。

◇ 開始する cap 、終了する cap の番号を入力して下さい。

開始： 0 終了： 19 0～19 で、20file 約 200万 packet ③

開始する cap（最初は、0 になります）の 数、
終了する cap の数を入力します。

※ 終了する cap 数の file がない場合は、検索処理自体は行えますが、
キャプチャーデータの終了時刻が正しく表示されません。

◇ 検索するTOPの件数 30 ④

結果として表示される 件数 を指定します。
この数が多くなると、処理の時間も長くなります。

※ 処理のアルゴリズムとしては、
まず、1つ目のfile で、TOP 件数分を抽出し、
次に 2つ目のfile で、TOP 件数分を抽出し、データを加算していきます。
最後の file までこれを続けます。
よって、TOP の件数を増やせば精度が上がりますが、処理時間は長くなります。

⑤
◇ 出力内容 ☑ 発IP ☐ 着IP ☐ 発プロトコル ☐ 着プロトコル

出力する項目を選択します。複数の項目の選択が可能ですが、
複数を選択すると 複数選択は、処理時間が長くなります。
2項目の場合は、1項目の2倍の時間がかかります。

◇ 絞込 ⑥ 例：特定のIP 10.0.1.14 or https 等

絞込を行う場合に入力します。
入力されたものが、ipアドレスであれば、 ipアドレス で絞込検索を行います。
ipアドレスではない場合は、 単なる パターンマッチングになります。
https と入力すると キャプチャーlog内に、 https の文字があれば、該当します。
10.0.1. と入力すると、これは ipアドレスではありませんので、この文字があるものが抽出されます。おおよそ、10.0.1.xx の nwアドレスを指定したのとほぼ同じ結果となります。

2. 検索結果例　その1

赤点線枠で選択した内容で検索した結果です。
renzoku_0 のため、正に今通信をしている状況の把握が可能です。

元となる cap ファイル： **renzoku_0.cap**
開始～終了 capファイル： **0 ～ 14**　【ファイル数：15　約 150 万packet】
検索するTOPの件数： **30**
出力内容： **発IP　着IP　発プロトコル　着プロトコル**

パケット時間帯：2023-02-04 16:08:35 ～ 2023-02-05 12:17:06 【 72511 秒 = 1208 分 31 秒 】

暫くお待ち下さい。20file 30項目出力で、 1出力当たり 約20秒かかります。　グラフは、TOP 10 までと その他の %です。

No	発IP	packet数	%
1	15[redacted]14	363370	52.6
2	12[redacted]74	122222	17.7
3	16[redacted]42	35558	5.2
4	10[redacted]00	33518	4.9
5	21[redacted]10	23207	3.4
6	52[redacted]32	15819	2.3
7	1[redacted]2	14576	2.1
30	18[redacted]23	962	0.1
-	others total	7357	1.1

No	着IP	packet数	%
1	15[redacted]14	340675	49.6
2	12[redacted]74	116157	16.9
3	16[redacted]242	36102	5.3
4	10[redacted]200	32709	4.8
5	21[redacted].10	23211	3.4
6	1[redacted].2	15251	2.2
7	52[redacted].32	15130	2.2
30	18[redacted]51	1196	0.2
-	others total	10000	1.5

No	発プロトコル	packet数	%
1		262732	53.6
2	https	166619	34.0
3	domain	30037	6.1
4	http	10303	2.1
5	ssh	8320	1.7

No	着プロトコル	packet数	%
1		262742	51.7
2	https	176207	34.6
3	domain	34375	6.8
4	ssh	9870	1.9
5	http	5026	1.0

この例では、15ファイル分の検索を行っています。
【　】内は、検索時間帯ですが、試験サイトのため、長い時間となっています。
通常は、 110万packetの場合数十秒程度です。
プロトコルの空欄は、ICMPです。 試験サイトのため、ICMPが多くなっています。

2. 検索結果例　その2　　機器AのIP　で絞込

赤点線枠で選択した内容で検索した結果です。
この例では、ある ip で絞込を行っています。

元となる cap ファイル： **renzoku_0.cap**
開始～終了 capファイル： **0 ～ 14**　【ファイル数：15　約 150 万packet】
検索するTOPの件数： **30**
出力内容： **発IP　着IP　発プロトコル　着プロトコル**
絞込：　**機器AのIP**
パケット時間帯：2023-02-04 16:08:35 ～ 2023-02-05 12:25:32 【 73017 秒 = 1216 分 57 秒 】

暫くお待ち下さい。20file 30項目出力で、 1 出力当たり 約20秒かかります。　　グラフは、TOP 10 までと その他の %です。

No	発IP	packet数	%
1	機器AのIP	123070	51.3
2	機器B	116956	48.7
-	others total	0	0.0

No	着IP	packet数	%
1	機器B	123072	51.3
2	機器AのIP	116958	48.7
-	others total	0	0.0

No	発プロトコル	packet数	%
1		151498	76.9
2	https	41212	20.9
3	64033	36	0.0

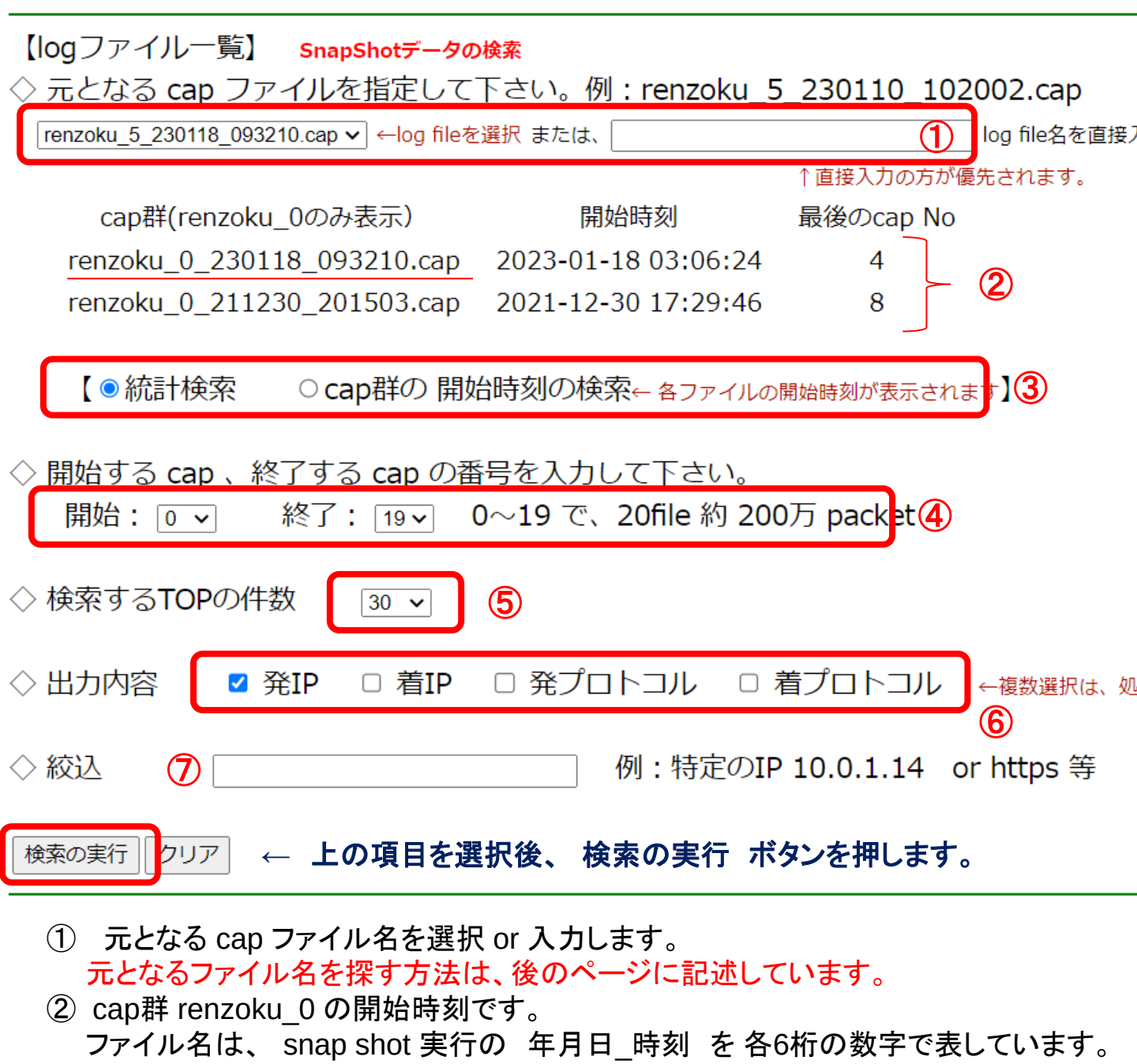
No	着プロトコル	packet数	%
1		151508	74.6
2	https	47335	23.3
3	64016	25	0.0

この例は、機器AのIP　で絞り込んだ例です。

機器Aは、機器Bとのみ通信を行っていて、プロトコルは https と ICMP であることが分かります。（試験サイトのため、ICMPが多くなっています）

3. Snap Shot データの検索

P4　検索3　のTOP画面で　**SnapShotデータ検索**　をクリックします。



① 元となる cap ファイル名を選択 or 入力します。
元となるファイル名を探す方法は、後のページに記述しています。

② cap群 renzoku_0 の開始時刻です。
ファイル名は、 snap shot 実行の 年月日_時刻 を 各6桁の数字で表しています。
230118 ⇒ 2023年1月18日　　093210 ⇒ 09:32:10

③ 統計検索 or cap群の開始時刻の検索 を選択します。
開始時刻の検索例は、後のページに記述しています。

④ 参照する cap ファイルの最初と最後を指定します。
ファイル数が多くなると、検索時間が長くなります。

⑤ 検索するTOPの件数を指定します。

⑥ 出力内容を選択します。複数選択時は時間が長くなります。

⑦ 絞込を行う時に入力します。

パケットキャプチャ-の検索結果のページ

ひとつ前に戻る　現在の時刻 ： 12:41:26

元となる cap ファイル： **renzoku_4_230110_102002.cap**
開始～終了 capファイル： **0 ～ 9**　【ファイル数：10　約 100 万packet】
検索するTOPの件数： **30**
出力内容： **発IP　着IP　発プロトコル　着プロトコル**
パケット時間帯：2023-01-10 09:38:50 ～ 2023-01-10 09:40:32 【 102 秒 = 1 分 42 秒 】

暫くお待ち下さい。20file 30項目出力で、１出力当たり 約20秒かかります。　グラフは、TOP 10 までと その他の %です。

No	発IP	packet数	%
1	17[redacted]50	83446	16.8
2	17[redacted]57	43097	8.7
3	52.[redacted]132	25304	5.1
4	17[redacted]33	18162	3.6
5	5[redacted]4	16277	3.3
6	17[redacted]32	16242	3.3
7	4[redacted]2	15845	3.2
8	4[redacted]0	14694	3.0
9	17[redacted]07	14577	2.9

No	発プロトコル	packet数	%
1	https	348505	53.3
2	[redacted]	45255	6.9
3	microsoft-ds	24198	3.7
4	http	19899	3.0
5	43438	18434	2.8

No	着IP	packet数	%
1	1[redacted]50	89284	16.9
2	17[redacted]57	61143	11.6
3	17[redacted]07	27178	5.2
4	1[redacted]04	20717	3.9
5	17[redacted]33	17488	3.3
6	52[redacted]132	16870	3.2
7	1[redacted]32	16553	3.1
8	5[redacted]4	15879	3.0
9	4[redacted]0	13934	2.6

No	着プロトコル	packet数	%
1	https	353286	51.5
2	[redacted]t	64002	9.3
3	38002	26254	3.8
4	47814	23686	3.5
5	microsoft-ds	21205	3.1

この例は、100万パケットで、約 1分 42秒です。
実サイトのため、試験サイトよりかなりのパケット量です。

次のページは、発IPの一番多いIPで絞り込んだ例です。

4. 検索結果例　その2　（snap shot）機器AのIP　で絞込

元となる cap ファイル： **renzoku_4_230110_102002.cap**
開始～終了 capファイル： **0 ～ 9**　【ファイル数：10　約 100 万packet】
検索するTOPの件数： **30**
出力内容： **発IP　着IP　発プロトコル　着プロトコル**
絞込：　**機器AのIP**
パケット時間帯：2023-01-10 09:38:50 ～ 2023-01-10 09:40:32 【 102 秒 = 1 分 42 秒 】

暫くお待ち下さい。20file 30項目出力で、１出力当たり 約20秒かかります。　グラフは、TOP 10 までと その他の %です。

No	発IP	packet数	%
1	機器AのIP	83446	49.6
2	Microsoft	24386	14.5
3	Microsoft	13420	8.0
4	機器B	9593	5.7
5	Microsoft	7132	4.2
6	Microsoft	7006	4.2
7	Microsoft	3691	2.2
8	Microsoft	3664	2.2

No	着IP	packet数	%
1	機器AのIP	89284	53.4
2	機器B	18509	11.1
3	Microsoft	15967	9.6
4	Microsoft	12321	7.4
5	Microsoft	6907	4.1
6	Microsoft	2914	1.7
7	機器C	2772	1.7
8	機器D	1941	1.2

No	発プロトコル	packet数	%
1	https	65664	41.1
2	43438	18434	11.5
3	47814	15582	9.8
4	38002	9533	6.0

No	着プロトコル	packet数	%
1	https	50881	31.5
2	47814	23686	14.7
3	38002	18434	11.4
4	43438	9533	5.9

この例は、機器Aは、Microsoft との通信が多いのが分かります。
プロトコルは、https です。

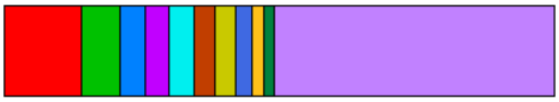
4. 検索結果例　その3　（snap shot） https で絞込

パケットキャプチャ-の検索結果のページ

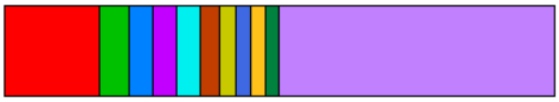
ひとつ前に戻る　　現在の時刻 ： 13:05:45

元となる cap ファイル： **renzoku_4_230110_102002.cap**
開始～終了 capファイル： **0 ～ 9**　【ファイル数：10　約 100 万packet】
検索するTOPの件数： **30**
出力内容： **発IP　着IP　発プロトコル　着プロトコル**
絞込： **https**
パケット時間帯：2023-01-10 09:38:50 ～ 2023-01-10 09:40:32 【 102 秒 = 1 分 42 秒 】

暫くお待ち下さい。20file 30項目出力で、1出力当たり 約20秒かかります。　　グラフは、TOP 10 までと その他の %です。



No	発IP	packet数	%
1	1[redacted]50	50887	14.0
2	52[redacted]32	25304	7.0
3	[redacted]4	16277	4.5
4	1[redacted]2	16242	4.5
5	[redacted]2	15845	4.4
6	[redacted]0	14694	4.0
7	1[redacted]4	13837	3.8
8	1[redacted]3	10016	2.8
30	5[redacted]10	2911	0.8
-	others total	99354	27.3



No	着IP	packet数	%
1	1[redacted]50	65668	17.2
2	[redacted]4	20717	5.4
3	52[redacted]32	16870	4.4
4	[redacted]2	16553	4.3
5	[redacted]4	15879	4.2
6	[redacted]0	13934	3.6
7	[redacted]2	10810	2.8
8	[redacted]6	10788	2.8
30	[redacted]8	2820	0.7
-	others total	105374	27.6

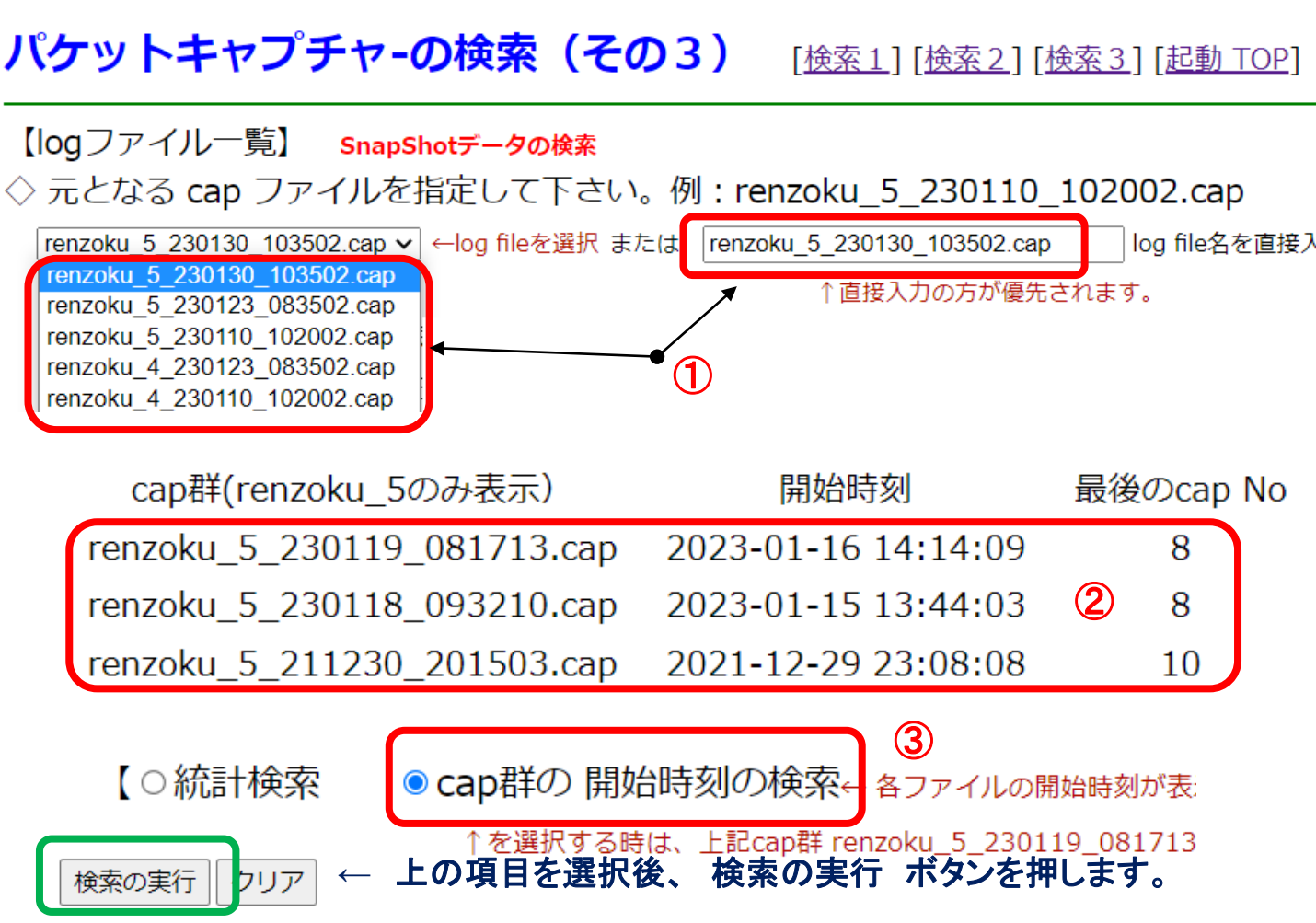
No	発プロトコル	packet数	%
1	https	348505	71.3
2	47814	15582	3.2
3	51052	6511	1.3
4	51595	6297	1.3

No	着プロトコル	packet数	%
1	https	353286	67.8
2	47814	23686	4.5
3	51595	5228	1.0
4	51052	5009	1.0

この例は、https で絞り込んだ例です。
帯グラフ の 紫部分（11位以下の合計）が半分近くありますので
https の通信は多くの機器が利用していることが分かります。

cap群の 開始時刻の検索の例です。

検索のため、どのファイルを指定したら良いかを知るために、
各ファイルの開始時刻を表示する方法を示します。



① 元となる cap ファイル名を選択 or 入力します。
② 過去に snap shot を行った renzoku_5（最初の時刻）の一覧です。
　上記の例では、過去に　3回の snap shot を行ったことが分かります。
③ cap群の 開始時刻の検索を選択します。

上記の条件の検索結果を次ページに示します。

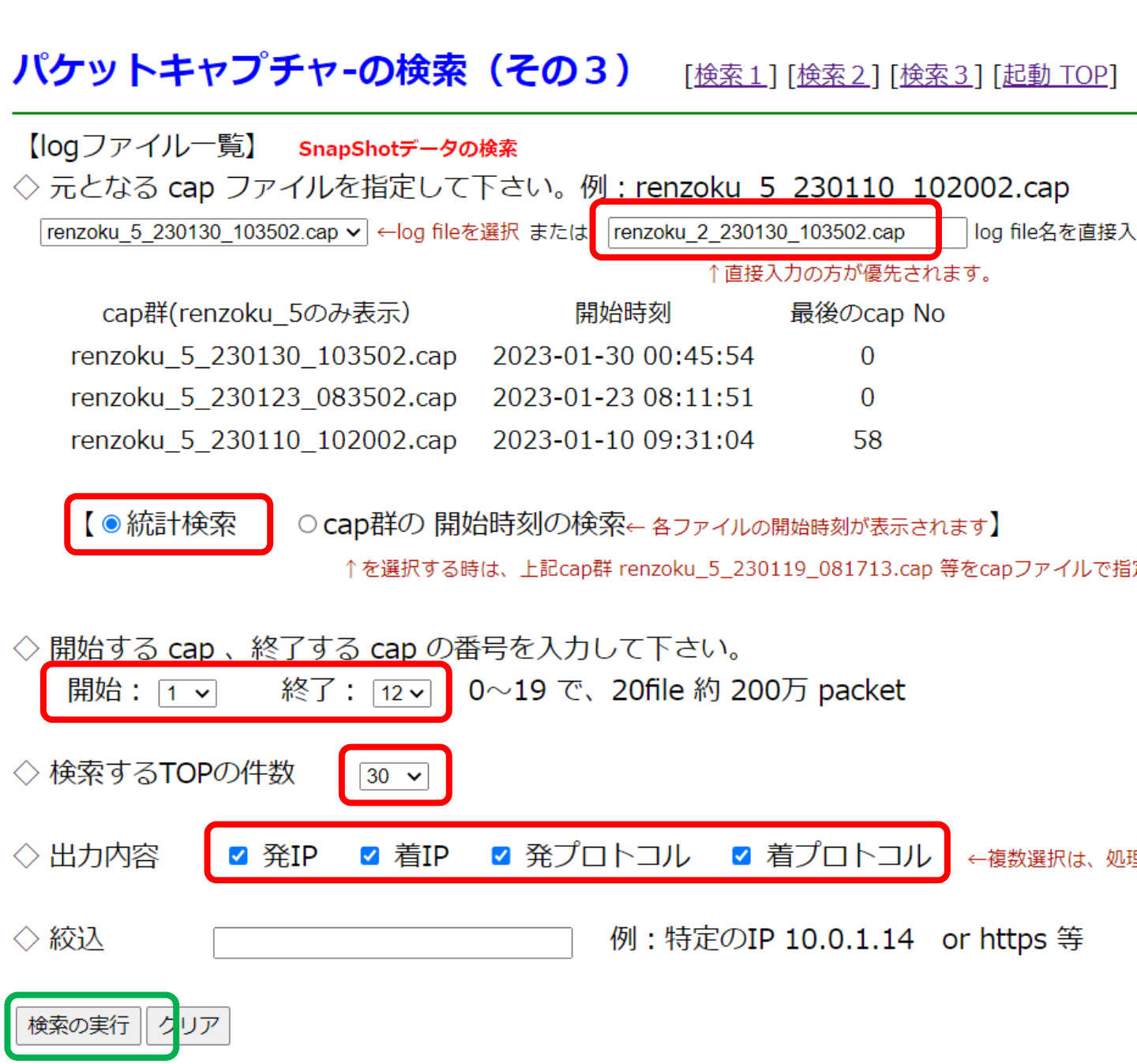
元となる cap ファイル： renzoku_5_230130_103502.cap

cap群の 開始時刻の検索

No	ファイル名	開始時刻
1	renzoku_5_230130_103502.cap	2023-01-30 00:45:54
	renzoku_2_230130_103502.cap	2023-01-30 08:25:08
	renzoku_2_230130_103502.cap1	2023-01-30 08:25:26
	renzoku_2_230130_103502.cap2	2023-01-30 08:26:11
	renzoku_2_230130_103502.cap3	2023-01-30 08:26:50
	renzoku_2_230130_103502.cap4	2023-01-30 08:27:22
	renzoku_2_230130_103502.cap5	2023-01-30 08:27:40
	renzoku_2_230130_103502.cap6	2023-01-30 08:28:02
	renzoku_2_230130_103502.cap7	2023-01-30 08:28:20
	renzoku_2_230130_103502.cap8	2023-01-30 08:29:03
	renzoku_2_230130_103502.cap9	2023-01-30 08:30:25
	renzoku_2_230130_103502.cap10	2023-01-30 08:30:52
	renzoku_2_230130_103502.cap11	2023-01-30 08:32:00
	renzoku_2_230130_103502.cap12	2023-01-30 08:34:34
	renzoku_2_230130_103502.cap13	2023-01-30 08:35:08
	renzoku_2_230130_103502.cap14	2023-01-30 08:36:10
	renzoku_2_230130_103502.cap15	2023-01-30 08:37:29
	renzoku_2_230130_103502.cap16	2023-01-30 08:38:39

元となる cap ファイル： renzoku_5_230130_103502.cap
の renzoku_5, renzoku_4, ～ renzoku_1, renzoku_0
5世代 4世代 1世代 0世代
の各ファイルの 開始時刻を表示します。
renzoku_5（5世代）が、一番古いデータになります。
renzoku_0 は、取得中の世代であり、cap 数が少ないことが普通です。

⇒ この検索により、調べたい時刻のファイルを抽出することが可能です。
例 8:26～8:30 までのデータを検索したい場合は、赤線矢印の
renzoku_2_230130_103502.cap 群の cap1 ～ cap12 を指定します。



前のページで抽出した、時間帯の検索を行います。
8:26～8:30 までのデータを検索したい場合は、赤線矢印の
renzoku_2_230130_103502.cap 群の cap1 ～ cap12 を指定します。

パケットキャプチャ-の検索結果のページ

ひとつ前に戻る

現在の時刻 ： 11:50:28

元となる cap ファイル： **renzoku_2_230130_103502.cap**
開始～終了 capファイル： **1 ～ 12** 【ファイル数：12 約 120 万packet】
検索するTOPの件数： **30**
出力内容： **発IP 着IP 発プロトコル 着プロトコル**
パケット時間帯：2023-01-30 08:25:26 ～ 2023-01-30 08:35:08 【 582 秒 = 9 分 42 秒 】

暫くお待ち下さい。20file 30項目出力で、1出力当たり 約20秒かかります。 グラフは、TOP 10 までと その他の %です。

No	発IP	packet数	%
1	2[redacted]35	121727	12.2
2	1[redacted]53	87871	8.8
3	19[redacted].20	74172	7.4
4	2[redacted]41	65434	6.5
5	19[redacted]171	61218	6.1
6	19[redacted]0.1	56972	5.7
7	1[redacted]55	48584	4.9
8	1[redacted]9	31003	3.1
9	19[redacted]111	25202	2.5
10	2[redacted]34	24150	2.4
11	1[redacted]8	24021	2.4
30	1[redacted]26	6428	0.6
-	others total	160918	16.1

No	着IP	packet数	%
1	2[redacted]5	106461	10.5
2	1[redacted]3	100373	9.9
3	19[redacted]71	74217	7.3
4	19[redacted].1	62572	6.2
5	19[redacted]20	61214	6.1
6	1[redacted]5	57969	5.7
7	2[redacted]1	54811	5.4
8	19[redacted].8	43658	4.3
9	15[redacted]02	28874	2.9
10	1[redacted]9	28789	2.8
11	19[redacted]11	27982	2.8
30	19[redacted].4	5489	0.5
-	others total	144014	14.2

No	発プロトコル	packet数	%
1	http	226075	22.5
2	https	153220	15.2
3	[redacted]	80389	8.0
4	20655	61198	6.1
5	microsoft-ds	59100	5.9

No	着プロトコル	packet数	%
1	http	201147	19.6
2	https	177503	17.3
3	microsoft-ds	82745	8.1
4	20655	74133	7.2
5	[redacted]	63122	6.1