パケットキャプチャーツール

ITSRecorder

1．パケットキャプチャーの問題点

トラブルの深い分析には、パケットキャプチャーが有効です。

パケットキャプチャーをするには、技術者が現場まで行き、問題の事象が発生するタイミングでキャプチャーすることが必要です。

折角現場に技術者が行っても現象が発生しない場合があり、

・稼働面の無駄

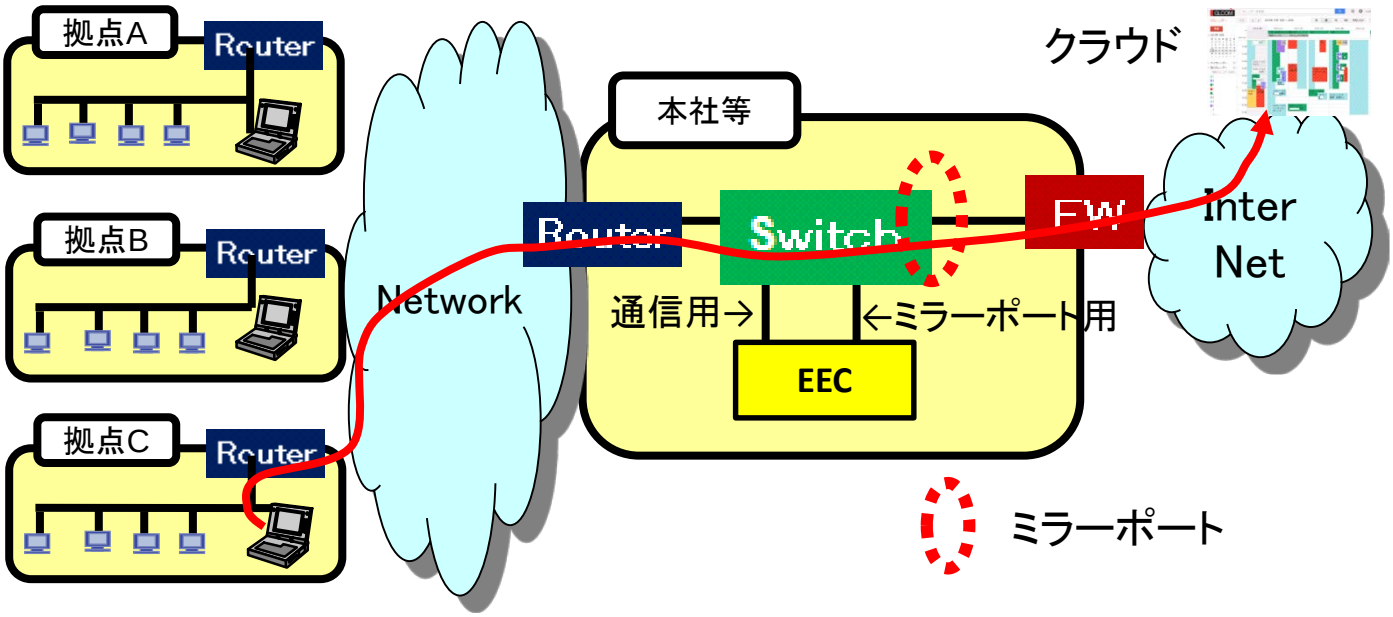
・問題発見に時間がかかる

といった問題があります。

今回、EEC（End to End Checker）に機能を追加し、遠隔にてお客さま自身がパケットキャプチャーを起動することにより、パケットの取得を実現しました。

2．構成例

パケットキャプチャーを行う場合には、事前に、取得したい機器にミラーポートを設定しておくことが必要です。



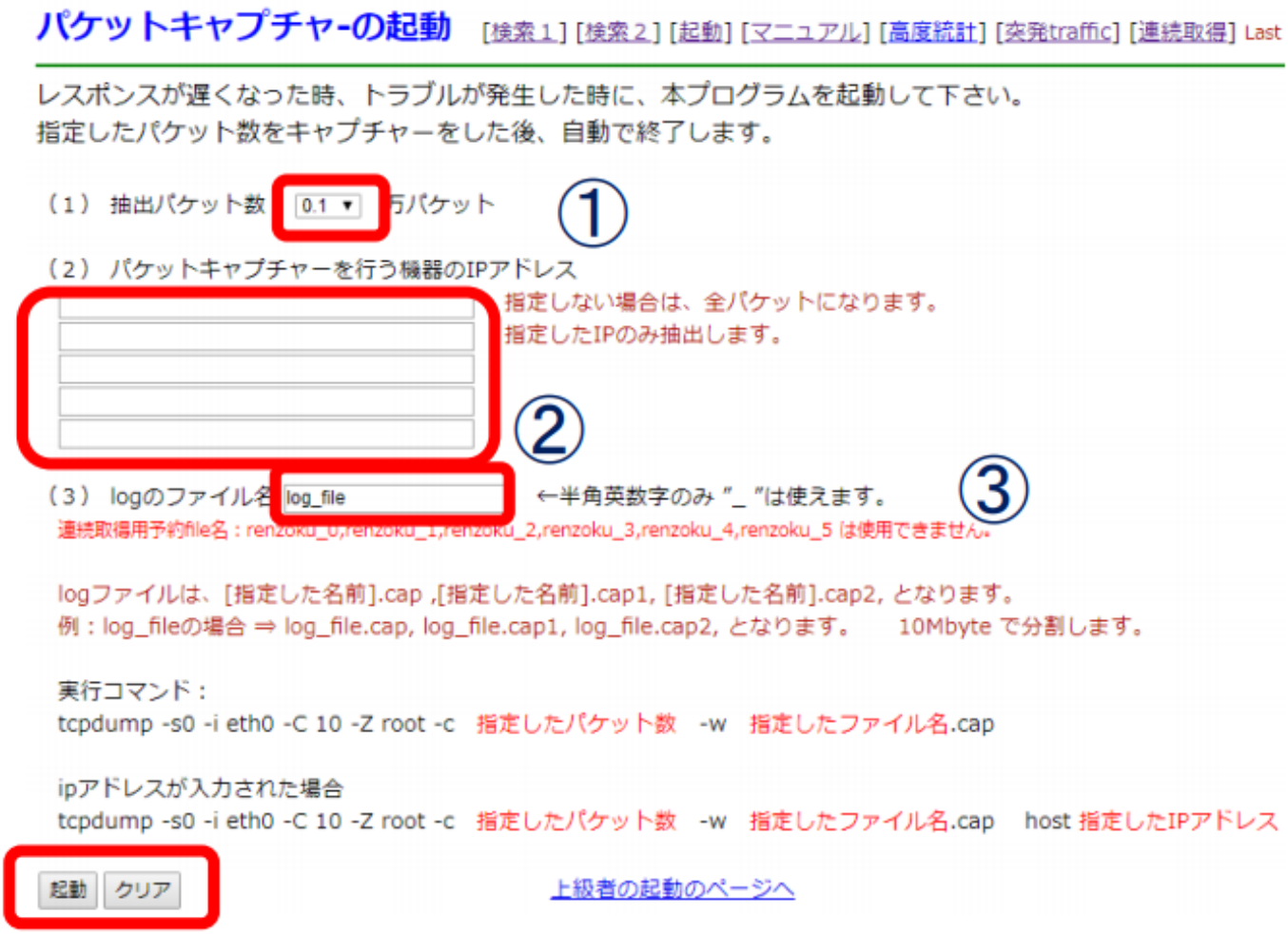
遠隔にてパケットキャプチャーの起動、パケットの取得、取得したデータの入手のため、EECには、2つのネットワークインタフェースが必要となります。

1つがミラーポート用で、もう1つがEECとの通信用です。

同じネットワークの端末から、EECにアクセスして、

ブラウザ上から、パケットキャプチャーの起動、停止、簡易分析、データの入手を行うことが可能です。

3. パケットキャプチャーの遠隔での起動



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。

パケットキャプチャーを取得しながら、次ページの簡易検索(分析）が可能ですので、タイムリーな問題解決に貢献できます。
また、取得したパケットキャプチャーのデータは、wireshark でも読むことができます。

5. パケットキャプチャーデータの簡易検索例

検索結果 検索キー(1)： 検索キー(2)： 検索キー(3)： 1 番目から表示

```
1  15:16:23.141544 IP 12[redacted].61180 > 13[redacted]74.http: Flags [.], ack 708505585, win 64,
2  15:16:23.467767 IP 12[redacted].61181 > 13[redacted]74.http: Flags [S], seq 125956141, win 175
3  15:16:23.467840 IP 13[redacted]74.http > 1[redacted].61181: Flags [S.], seq 3159924227, ack 1
4  15:16:23.494409 IP 12[redacted].61181 > 13[redacted]74.http: Flags [.], ack 1, win 68, length
5  15:16:23.501054 IP 12[redacted].61181 > 13[redacted]74.http: Flags [P.], seq 1:426, ack 1, win
6  15:16:23.501124 IP 13[redacted]74.http > 1[redacted].61181: Flags [.], ack 426, win 245, lengt
7  15:16:23.547747 IP 13[redacted]74.http > 1[redacted].61181: Flags [.], seq 1:1415, ack 426, w
8  15:16:23.547789 IP 13[redacted]74.http > 1[redacted].61181: Flags [P.], seq 1415:2693, ack 42
9  15:16:23.549234 IP 13[redacted]74.http > 1[redacted].61181: Flags [P.], seq 2693:2698, ack 42
10 15:16:23.549316 IP 1[redacted]174.http > [redacted]07.61181: Flags [F.], seq 2698, ack 426, w
11 15:16:23.577565 IP 1[redacted]07.61181 > 1[redacted]74.http: Flags [.], ack 2698, win 68, leng
12 15:16:23.577610 IP 1[redacted]07.61181 > 1[redacted]74.http: Flags [.], ack 2699, win 68, leng
13 15:16:23.581015 IP 1[redacted]07.61181 > 1[redacted]74.http: Flags [R.], seq 426, ack 2699, w
14 15:16:23.585971 IP 1[redacted]07.61182 > 1[redacted]74.http: Flags [S], seq 1429686267, win 1
15 15:16:23.586018 IP 1[redacted]174.http > [redacted]07.61182: Flags [S.], seq 4274149018, ack
16 15:16:23.586325 IP 1[redacted]07.61183 > 1[redacted]74.http: Flags [S], seq 1106109216, win 1
17 15:16:23.586353 IP 1[redacted]174.http > [redacted]07.61183: Flags [S.], seq 3336183080, ack
18 15:16:23.587307 IP 1[redacted]07.61184 > 1[redacted]74.http: Flags [S], seq 1647774341, win 1
19 15:16:23.587335 IP 1[redacted]174.http > [redacted]07.61184: Flags [S.], seq 1991678626, ack
20 15:16:23.587945 IP 12[redacted]07.61185 > 13[redacted]174.http: Flags [S], seq 2507270753, win 1
```

IPプレトコルのポート種別の一覧

【送信元】

1	.http	29306
2	.blp1	3801
3	.https	2353
4	.microsoft-ds	2166
5	.cypress	1203
6	.servexec	631
7	.ms-sql-s	626
8	.personal-agent	620
9	.glogger	580
10	.capwap-data	412

【送信先】

1	.http:	31160
2	.snmp:	9648
3	.blp1:	4609
4	.microsoft-ds:	2873
5	.jetdirect:	2413
6	.https:	2349
7	.cypress:	981
8	.ms-sql-s:	816
9	.personal-agent:	763
10	.servexec:	479

IPアドレス(Top30)

【送信元】

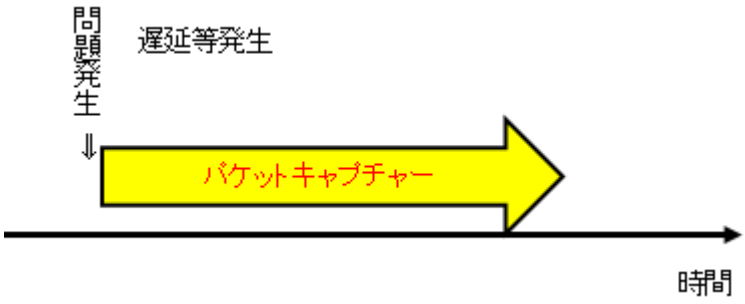
1	10[redacted]0.10	12264
2	10[redacted]50.15	11337
3	10[redacted]190.59	5870
4	10[redacted]0.140	3825
5	10[redacted]5	2935
6	10[redacted]50.1	2343
7	10[redacted]210.12	2250
8	10[redacted]0.200	1911
9	10[redacted]3	1626
10	10[redacted]38	1536

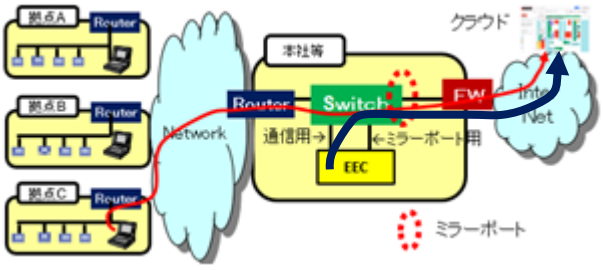
【送信先】

1	10[redacted]0.10	14242
2	1[redacted]50.15	10206
3	1[redacted]190.59	5399
4	1[redacted]0.140	4613
5	1[redacted]210.12	2934
6	1[redacted]50.1	2451
7	1[redacted]5	2251
8	1[redacted]	2022
9	1[redacted]0.200	1921
10	10[redacted]0.1	1759

パケットキャプチャーツール

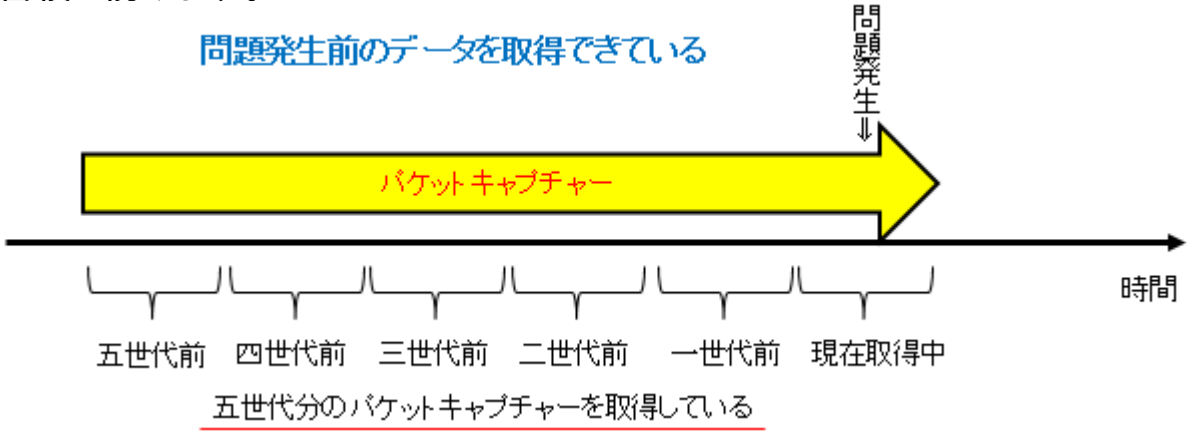
6. 突発トラヒック時のパケットデータの取得
　EECは、ping、http試験等を行い、そのレスポンスの値を把握しています。
例えば、あるWEBサイトのアクセスで遅延が生じた時に、パケットキャプチャーを起動することが可能です。





この試験で遅延が発生した場合にパケットキャプチャーを開始

7. 連続してパケットデータを取得
　「6. 突発トラヒック時」が生じる前のデータを入手することも可能です。
指定したパケットキャプチャー数（例500万パケット）を連続して取得し、そのデータを五世代分、蓄積します。
　蓄積データは、サイクリックに蓄積を行いますので、
　・現在の取得中のデータファイル
　・一世代前～五世代前のデータファイル
　を蓄積し続けます。



＊スナップショット機能により、ブラウザ上から、5世代のデータのコピーを取ることが可能です。

① 遠隔によるパケットキャプチャーの制御
② 突発トラヒック（遅延発生時等）時のパケットキャプチャーの起動
③ 連続してパケットキャプチャーの取得
　上記により、パケットキャプチャーを効率的に実施することができ、トラブルの原因究明に貢献することができます。