○○○○○株式会社 御中

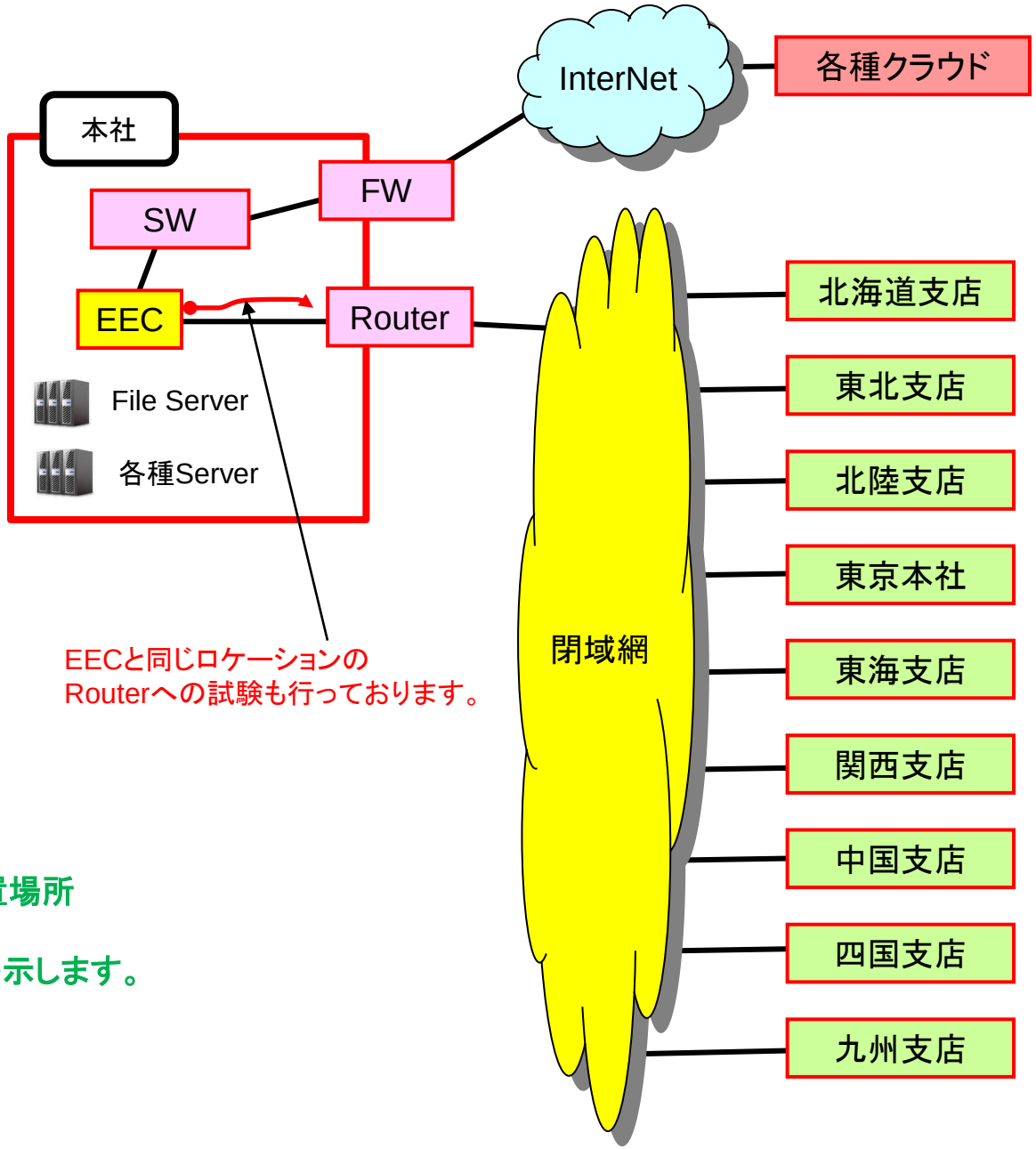
アクションレポート（2023年08期）

通常、アクションレポートは3ヶ月に1回の作成を目安としております。
今回は、2023.6.1～8.31 にデータを中心にまとめました。
本レポートを元に、オンラインクリニック（Action Reportの説明のWEB会議）で詳細説明を行います。
オンラインクリニックのスケジューリングをお願いします。

【目次】

アイティエスコンサルティング株式会社
2023/ 09/ xx

1. EECの設置場所と全体構成



EECの設置場所

全体構成を示します。

2. 監視登録情報

[01][02][03][04][05][06][07][08][09][10]　国内網_Ping監視(g1 : 9 拠点)

-	IP Address	場所	-	IP Address	場所	-	IP Address	場所	-	IP Address	場所
○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]
○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]
○	[redacted]	[redacted]									

[01][02][03][04][05][06][07][08][09][10]　InterNet上のサーバ_Pin監視(g4 : 4 拠点)

-	IP Address	場所	-	IP Address	場所	-	IP Address	場所	-	IP Address	場所
○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]

[01][02][03][04][05][06][07][08][09][10]　Port試験　53port (g5 : 3 拠点)

-	IP Address	場所	-	IP Address	場所	-	IP Address	場所
○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]

[01][02][03][04][05][06][07][08][09][10]　https試験(g6 : 4 拠点)

-	IP Address	場所	-	IP Address	場所	-	IP Address	場所	-	IP Address	場所
○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]	○	[redacted]	[redacted]

EECでは、グループ毎に　試験内容、試験間隔、アラート時のメール送信の有無　を設定することができます。

3. アラート状況　回数まとめ　9月

回数まとめで、障害回数の多い機器、総連続回数が多い機器については注意が必要です。
原因を把握されていないアラートは特に注意が必要です。

◇ 2023年 09月

No	拠点名	グループ	IP	障害回数	総連続回数	種類
1	[redacted]	g6	[redacted]	16	81	遅延
2	[redacted]	g6	[redacted]	9	31	ダウン
3	[redacted]	g10	[redacted]	4	12	ダウン
4	[redacted]	g9	[redacted]	3	2977	ダウン
5	[redacted]	g6	[redacted]	2	9	ダウン
6	[redacted]	g9	[redacted]	2	9	ダウン
7	[redacted]	g6	[redacted]	2	8	遅延
8	[redacted]	g9	[redacted]	2	8	ダウン
9	[redacted]	g9	[redacted]	2	8	ダウン
10	[redacted]	g9	[redacted]	1	4	ダウン
11	[redacted]	g8	[redacted]	1	3	ダウン
12	[redacted]	g10	[redacted]	1	3	ダウン

上記の一覧は、お客様自身でも同様の検索が可能です。
お客様はお手元のPCより
http://EECのIPアドレス/50ping/log_bunseki/
にアクセスして下さい。

過去のデータに遡って、各種絞込検索が可能です。
ある機器（拠点）で、品質が向上しているか、していないか直ぐに分かります。

3. アラート状況　回数まとめ　8月

◇ 2023年 08月

No	拠点名	グループ	IP	障害回数	総連続回数	種類
1	[redacted]	g6	[redacted]	183	849	遅延
2	[redacted]	g8	[redacted]	44	4557	ダウン
3	[redacted]	g6	[redacted]	36	166	遅延
4	[redacted]	g6	[redacted]	17	90	遅延
5	[redacted]	g6	[redacted]	12	68	遅延
6	[redacted]	g6	[redacted]	5	23	ダウン
7	[redacted]	g6	[redacted]	4	18	ダウン
8	[redacted]	g6	[redacted]	2	12	ダウン
9	[redacted]	g6	[redacted]	2	12	ダウン
10	[redacted]	g9	[redacted]	2	6	ダウン
11	[redacted]	g9	[redacted]	1	17206	ダウン
12	[redacted]	g4	[redacted]	1	132	ダウン
13	[redacted]	g8	[redacted]	1	6	ダウン
14	[redacted]	g9	[redacted]	1	4	ダウン
15	[redacted]	g9	[redacted]	1	4	ダウン
16	[redacted]	g9	[redacted]	1	4	ダウン

3. アラート状況　回数まとめ　7月

◇ 2023年 07月

No	拠点名	グループ	IP	障害回数	総連続回数	種類
1	[redacted]	g6	[redacted]	84	316	遅延
2	[redacted]	g6	[redacted]	30	118	遅延
3	[redacted]	g6	[redacted]	9	30	遅延
4	[redacted]	g6	[redacted]	8	30	遅延
5	[redacted]	g6	[redacted]	8	26	ダウン
6	[redacted]	g6	[redacted]	1	3	ダウン
7	[redacted]	g1	[redacted]	1	3	ダウン

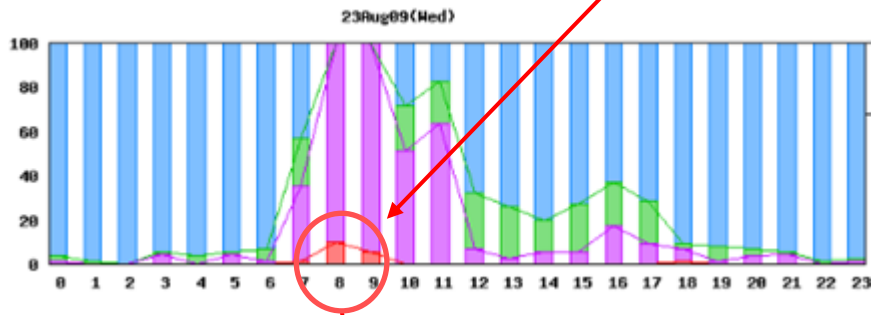
4. アラート詳細分析例　その1

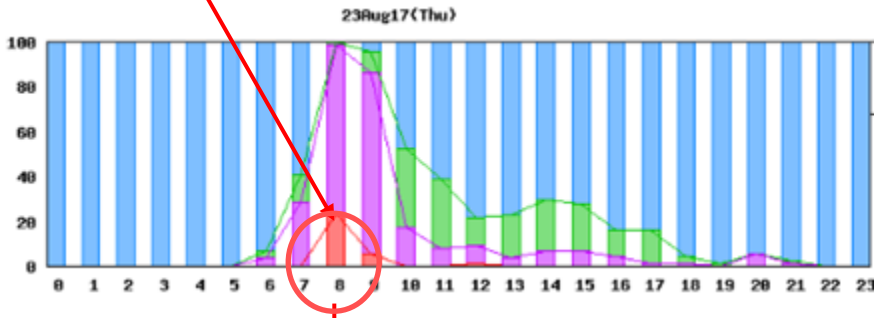
EECの遅延・timeout 状況、トラフィック状況から、帯域不足が考えられます。 **Action** ： 増速を依頼しております。
これまでの経験で、遅延が　timeout までになると、 エンドユーザ様のアプリで再送が多数発生し、
『非常に遅い』 との苦情に繋がります。

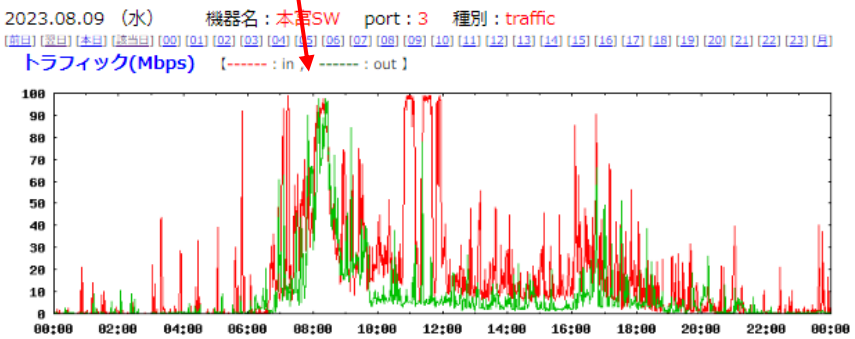
■Place=[redacted], IP=10.40.0.1, 年月=2023/08, Group=[redacted]

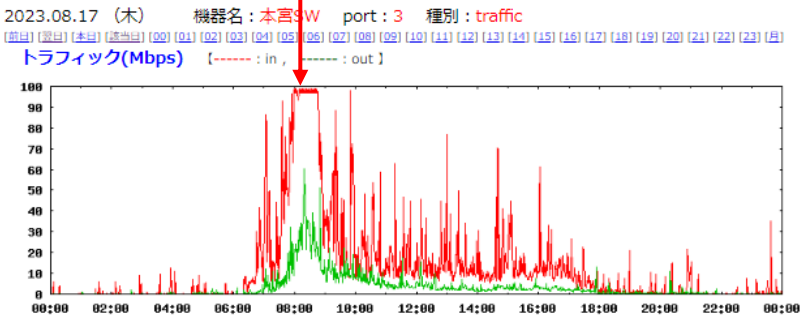
戻る　前の月　次の月　前の拠点　次の拠点

日の指定		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
種別	合計	火	水	木	金	土	日	月	火	水	木	金	土	日	月	火	水	木	金	土	日	月	火	水	木	金	土	日	月	火	水	木
Min	19.737(ms)	19.840	19.866	19.937	19.865	19.911	19.893	19.804	19.959	19.889	19.935	19.864	19.916	19.907	19.874	19.897	19.776	19.794	19.957	19.928	19.864	19.851	19.915	19.887	19.903	19.855	19.875	19.895	19.906	19.737	19.924	19.977
Max	350.630(ms)	63.884	61.343	76.780	67.191	47.695	40.376	75.634	74.709	150.738	89.863	43.167	54.514	52.045	63.165	32.059	52.400	134.870	97.845	53.163	45.087	93.831	76.604	90.359	350.630	104.356	47.073	31.708	77.810	84.845	54.604	60.184
Total	55433(回)	1788	1789	1788	1789	1788	1789	1788	1788	1784	1788	1789	1788	1789	1788	1789	1788	1785	1789	1788	1789	1789	1788	1788	1788	1788	1789	1789	1788	1788	1789	1788
平均	21.815(ms)	21.590	21.677	21.696	21.279	20.854	20.669	21.599	21.891	27.028	21.980	20.718	20.912	20.689	20.807	20.709	20.920	24.945	22.487	21.050	20.643	23.334	22.105	22.882	22.600	21.325	20.728	20.654	22.698	22.177	21.946	21.777
普通	48721(87.89%)	1539	1501	1531	1572	1751	1766	1519	1468	1280	1519	1753	1746	1762	1735	1733	1696	1414	1521	1695	1776	1368	1392	1372	1433	1558	1764	1761	1452	1460	1444	1440
少し遅い	4089(7.38%)	164	180	173	171	28	22	179	211	[redacted]	172	28	20	21	39	48	73	[redacted]	141	54	11	200	249	236	216	181	20	26	195	208	215	258
遅い	2529(4.56%)	83	103	82	45	9	1	84	107	304	93	7	22	6	14	8	19	186	124	38	2	214	144	177	132	47	5	2	138	117	130	86
timeout	94(0.17%)	2	5	2	1	0	0	6	2	13	4	1	0	0	0	0	0	22	3	1	0	7	3	3	7	2	0	0	3	3	0	4
不明	0(0.00%)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0









色々なお客様の分析例とActionについて記述しています。

4. アラート詳細分析例　その2

EECと同じロケーションのRouterの ping 試験で遅延が発生しています。
通常 0.6ms 程度の応答が、20ms を超える場合があります。
遅延時は、全地域との通信に影響があります。原因究明と対応が必要です。

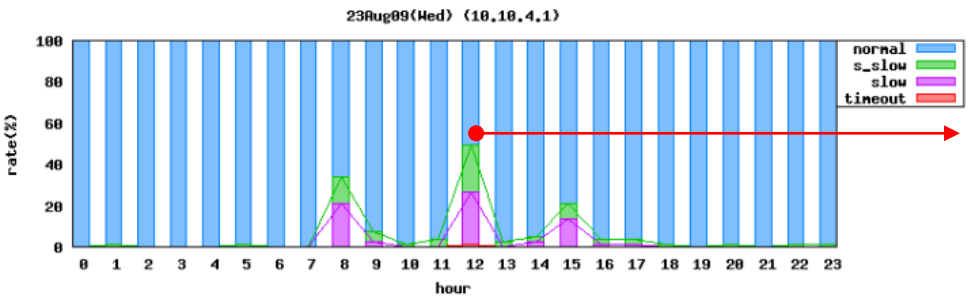
時刻毎のまとめ

■Place=本社Router_LAN側, IP=[redacted], 年月日=2023/08/09(水), Group=[redacted]見(g1)

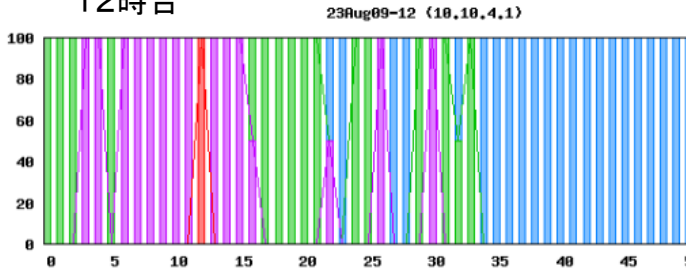
戻る　前の日　次の日　当月　前の拠点　次の拠点

時刻指定 / 種類	合計	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Min	0.423(ms)	0.622	0.632	0.640	0.646	0.622	0.624	0.624	0.621	0.656	0.629	0.609	0.620	0.628	0.603	0.630	0.603	0.628	0.633	0.637	0.423	0.605	0.619	0.622	0.643
Max	64.448(ms)	0.958	6.477	1.062	1.106	1.058	8.082	1.350	2.771	64.448	33.225	8.326	15.667	30.235	10.225	24.634	47.933	31.034	21.150	8.857	5.103	6.757	2.547	8.015	6.809
Total	1915(回)	80	79	80	80	80	80	80	79	80	80	80	80	79	79	80	80	80	80	80	79	80	80	80	80
平均	2.200(ms)	0.758	1.790	0.776	0.776	0.762	0.890	0.775	0.853	11.598	2.195	1.009	1.612	9.725	1.431	1.776	6.611	1.677	1.700	0.993	0.875	0.870	0.797	1.840	0.856
普通	1804(94.20%)	80	78	80	80	80	79	80	79	53	74	79	77	40	77	76	63	77	77	79	79	79	80	79	79
少し遅い	56(2.92%)	0	1	0	0	0	1	0	0	10	4	1	3	18	2	2	6	2	2	1	0	1	0	1	1
遅い	54(2.82%)	0	0	0	0	0	0	0	0	17	2	0	0	20	0	2	11	1	1	0	0	0	0	0	0
timeout	1(0.05%)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
不明	0(0.00%)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

□普通　：0.423　～6.423　(ms) (間隔：6.000 ms)
□少し遅い：6.423　～20.423　(ms) (間隔：14.000 ms)
□遅い　：20.423～1000.000 (ms) (間隔：979.577 ms)



12時台




```
12:00:44 : 8.977
12:01:29 : 7.808
12:02:14 : 8.091
12:03:00 : 24.860
12:03:45 : 23.376
12:04:31 : 21.374
12:05:17 : 19.363
12:06:04 : 23.095
12:06:51 : 24.860
12:07:39 : 22.166
12:08:26 : 24.083
12:09:13 : 22.971
12:09:59 : 21.461
12:10:46 : 23.705
12:11:32 : 22.650
12:12:18 : timeout
12:13:05 : 24.370
```

Action

この機器を別グループに登録し、試験間隔を短くします。
比較対象として、同じグループにRouterと同じトポロジーの機器を登録します。

Action　の結果

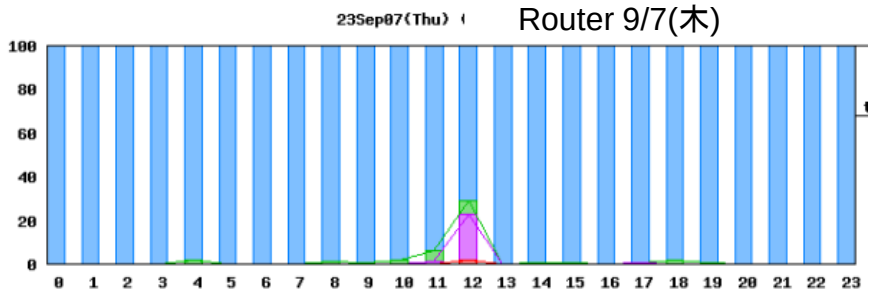
月の日毎の分布 グループ：特別監視(g10：4 拠点)

■場所指定[target_file順](Pingの過去の状況)　[IPソート] [拠点名ソート]

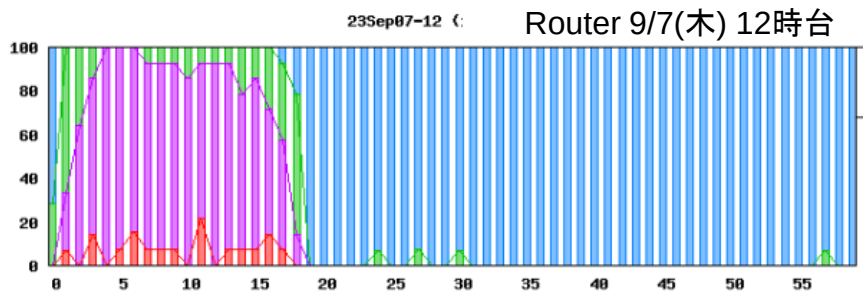
[01][02][03][04][05][06][07][08][09][10]

-	IP Address	場所	-	IP Address	場所	-	IP Address	場所	-	IP Address	場所
○	10[redacted]1	IX[redacted]er	○	[redacted]1	A[redacted]P	○	1[redacted]0	W[redacted]er	○	1[redacted]0	C[redacted]エア

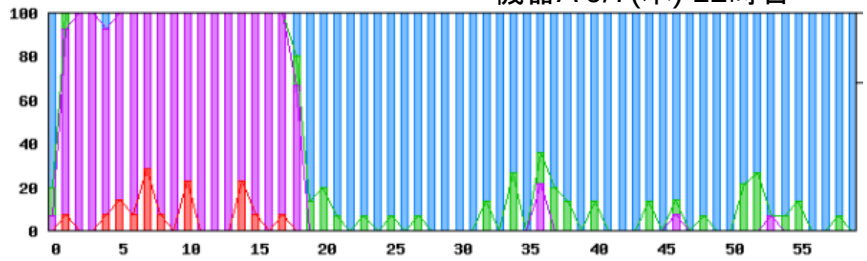
Router　機器A　機器B　機器C



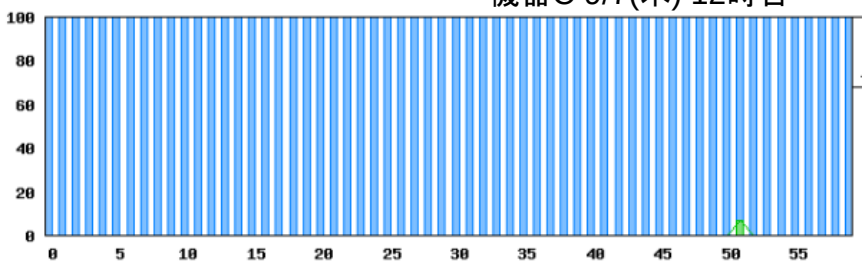
Router 9/7(木)



Router 9/7(木) 12時台



機器A 9/7(木) 12時台



機器C 9/7(木) 12時台

試験間隔を短くしたので、鮮明に 遅延、timeout の状況を把握することができるようになりました。
機器Aは遅延有り、機器Cはでは遅延がないことから、原因の絞り込みが深まります。

⇒ **次のActionとして**、①Routerのトラフィックの調査、②Routerのポイントでのパケットキャプチャーを推奨します。

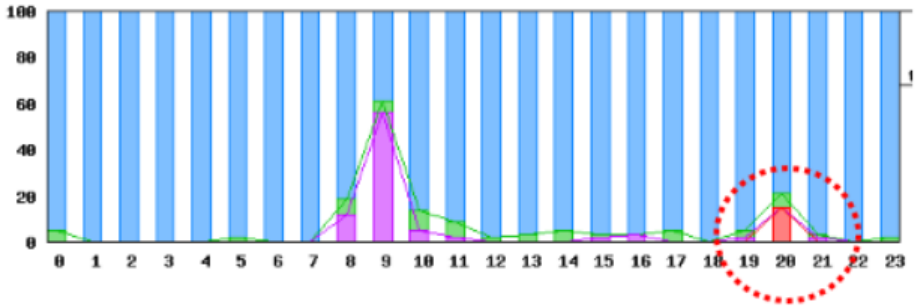
4. アラート詳細分析例　その2　補足

トラフィック増により、遅延・timeout が発生することがありますが、
トラフィックがなくても、遅延・timeoutがあることあります。注意が必要です。

帯域に余裕があるのにRouterが落ちる
https://its-consul.co.jp/itsr/router_down.html

Windows UPdateの後、あるサーバーが2,000の端末と無意味な通信（エラーパケット）が発生し、この拠点の全通信ができなくなりました。

お客様は、このあるサーバーについて、意識をされておりませんでした。



20:13:24 : 29.821
20:14:32 : 29.336
20:15:34 : 29.377
20:17:02 : timeout
20:18:24 : timeout+2
20:20:04 : timeout+3
20:21:55 : timeout+4
20:23:47 : timeout+5
20:25:37 : timeout+6
20:27:23 : timeout+7
20:29:10 : 29.081
20:30:16 : timeout
20:31:58 : 30.008
20:33:00 : 29.732

	IPアドレス	パケット数	%
1	Server-B	4,286,027	85.8
2	10.xxx.88.70	118,735	2.4
3	10.xxx.88.66	113,561	2.3
4	10.xxx.88.71	96,176	1.9
5	10.xxx.88.69	85,396	1.7
6	10.1.yyy.10	76,646	1.5
7	10.1.yyy.200	26,218	0.5
8	10.yyy.70.15	25,888	0.5
9	10.1.yyy.1	21,887	0.4
10	10.xxx.88.65	17,357	0.3

5. timeout 率　9月

No	拠点名	ping総数	timeout総数（内不明数）	timeout率（%）
1	[redacted]	29,332	3030(0)	10.33
2	[redacted]	24,543	184(0)	0.75
3	[redacted]	24,543	166(0)	0.676
4	[redacted]	29,429	150(0)	0.51
5	[redacted]	29,332	81(0)	0.276
6	[redacted]	29,332	68(0)	0.232
7	[redacted]	29,465	54(0)	0.183
8	[redacted]	24,543	41(0)	0.167
9	[redacted]	29,332	42(0)	0.143
10	[redacted]	28,099	34(0)	0.121
11	[redacted]	29,429	35(0)	0.119
12	[redacted]	29,465	35(0)	0.119
13	[redacted]	28,099	28(0)	0.1
14	[redacted]	28,099	28(0)	0.1
15	[redacted]	29,331	29(0)	0.099
16	[redacted]	29,440	28(0)	0.095
17	[redacted]	28,099	25(0)	0.089
18	[redacted]	28,099	25(0)	0.089
19	[redacted]	29,440	26(0)	0.088
20	[redacted]	29,465	25(0)	0.085
21	[redacted]	29,440	25(0)	0.085
22	[redacted]	28,099	23(0)	0.082
23	[redacted]	29,440	24(0)	0.082
24	[redacted]	29,473	23(0)	0.078

注意が必要です。

今までの経験値で、01 を超える場合は、注意が必要です。
通常 timeoutが3回で、アラートとなっていますが、timeout が 2回や、1回とアラートにならない機器で、潜在故障がある機器があります。

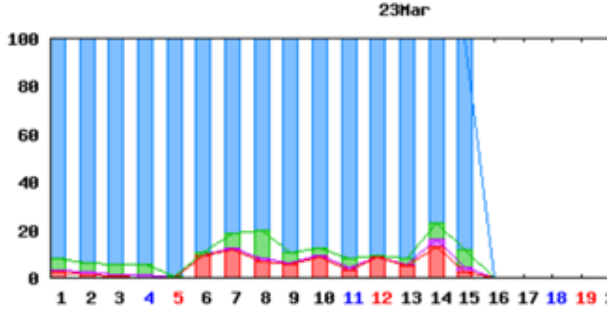
例：30秒止まることが、月に 6回程ある事象を過去に発見しております。

この分析、Action(試験間隔を短くする）例のようなトラブルを抽出することができます。

6. timeout 率　におけるActionの例

No	拠点名	group	ping総数	timeout総数（内不明数）	timeout率（%）
67	タイムレコーダーA	g21	48274	720(9)	1.491
86	タイムレコーダーB	g21	48274	200(9)	0.414
87	タイムレコーダーC	g21	48274	197(9)	0.408
98	タイムレコーダーD	g21	48274	166(9)	0.344

同じタイムレーコーダーですが、Aだけ、timeout が　かなり悪くなっています。詳細を分析しました。



平日は、かなりの timeout が発生しています。

日の指定		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
種類	合計	水	木	金	土	日	月	火	水	木	金	土	日	月	火	水
Min	16.752(ms)	16.846	16.802	16.822	16.810	16.788	16.752	16.851	16.835	16.856	16.757	16.850	16.798	16.788	16.832	16.849
Max	535.729(ms)	180.629	205.170	524.582	56.893	341.173	185.516	535.729	258.967	58.922	136.884	61.712	54.334	60.939	68.551	131.424
Total	24988(回)	1724	1724	1724	1725	1725	1722	1720	1722	1723	1721	1724	1722	1723	1721	868
平均	18.328(ms)	18.390	18.423	18.920	18.049	17.460	17.642	18.750	19.796	18.155	18.025	18.062	17.278	17.938	19.492	18.966
普通	22387(89.59%)	1583	1621	1630	1627	1713	1538	1404	1384	1546	1507	1589	1563	1590	1326	766
少し遅い	1043(4.17%)	87	62	72	82	7	26	101	200	66	54	63	6	37	118	62
遅い	221(0.88%)	14	19	12	11	2	3	10	20	16	11	19	1	16	51	16
timeout	1337(5.35%)	40	22	10	5	3	155	205	118	95	149	53	152	80	226	24

他の機器（良い機器）と比較することにより、潜在的なトラブルを発見することが可能です。

6. timeout 率 における Action 例

Action　お客様へ依頼

（1）タイムレコーダーA　のケーブル、接続Switch　の確認をお願いします。
　　※ケーブルの接続部分を強く押し入れる等の操作をお願いします。

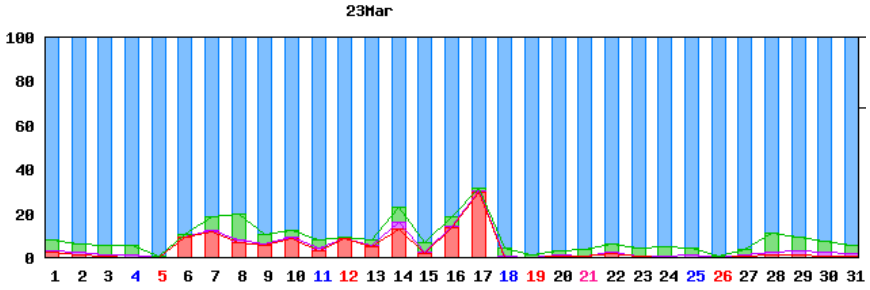
（1）で、回復しない場合は、
（2）タイムレコーダーA　と同じSwitchに接続されている機器（機器＋α）を監視に追加して下さい。
ケース1：タイムレコーダーA、 機器＋α　とも timeout の場合　⇒　Switch 等　共通機器の原因と考えられます。
ケース2：機器＋α　で timeoutがない場合は、
　　タイムレコーダーAの　単体の不良と考えられます。
　　予備のタイムレコーダーがあれば、それと交換をしてみて下さい。

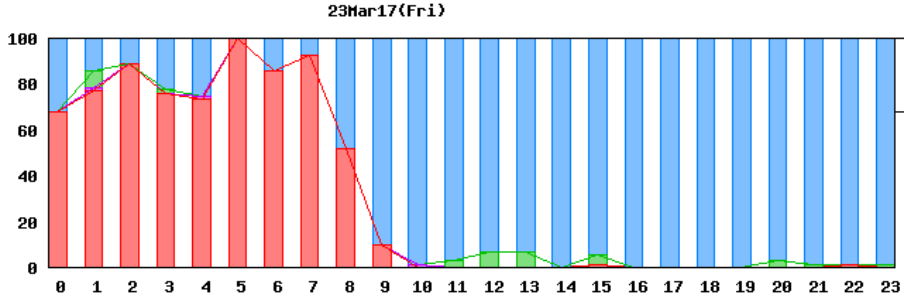
お客様でのAction結果

（1）タイムレコーダーAに接続するスイッチングハブが 老朽化しており、そのハブを新しいものに交換。

（2）ハブ間をカスケードしているケーブルのコネクタの爪が無く、抜けやすい状態であったため、LANケーブルを更新しました。

⇒　上記の対応で、timeout の発生がなくなりました。



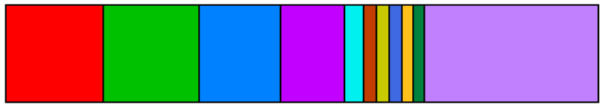


2023年3月に、徐々に timeout が増えていきました。
丁度、お客様の確認時には、timeout が激しくなりましたが、 タイムリーな対応を行った結果、
大事には至りませんでした。

7. パケットキャプチャ　サンプル分析

元となる cap ファイル： renzoku_1_230719_100813.cap
開始～終了 capファイル： 39 ～ 59 【ファイル数：21 約 210 万packet】
検索するTOPの件数： 30
パケット時間帯：2023-07-19 09:58:14 ～ 10:07:30【 556 秒 = 9 分 16 秒 】

両者間のパケット数が多くなっています。



No	発IP	packet数	%
1	機器A 本社機器 a	279526	16.8
2		254734	15.3
3		192844	11.6
4		91657	5.5
5		58851	3.5
6		49743	3.0
7		36590	2.2
8		33899	2.0
9		32008	1.9
10		31061	1.9
11		29982	1.8
12		28635	1.7
13		23470	1.4
14		21249	1.3
15		20470	1.2
16		19365	1.2
17		17275	1.0
18		17220	1.0
19		17016	1.0
20		16630	1.0

OCN

Level3

Microsoft

大塚商会
EdgeCast

No	着IP	packet数	%
1		339708	20.0
2	機器A 本社機器 a	280168	16.5
3		253697	14.9
4		67906	4.0
5		54519	3.2
6		53065	3.1
7		43433	2.6
8		33505	2.0
9		30359	1.8
10		29587	1.7
11		26735	1.6
12		24483	1.4
13		21333	1.3
14		19587	1.2
15		17150	1.0
16		17013	1.0
17		16066	0.9
18		15845	0.9
19		14838	0.9
20		13695	0.8

No	発プロトコル	packet数	%
1	4529	278879	16.5
2	pando-pub	272068	16.1
3	http	232092	13.7
4	https	184992	10.9
5	52300	54795	3.2
6	64714	36422	2.2
7	64717	35387	2.1
8	plethora	33956	2.0

No	着プロトコル	packet数	%
1	4529	253363	15.3
2	pando-pub	169282	10.2
3	https	121031	7.3
4	http	117515	7.1
5	52300	63662	3.8
6	64714	40211	2.4
7	64717	37857	2.3
8	50022	37136	2.2

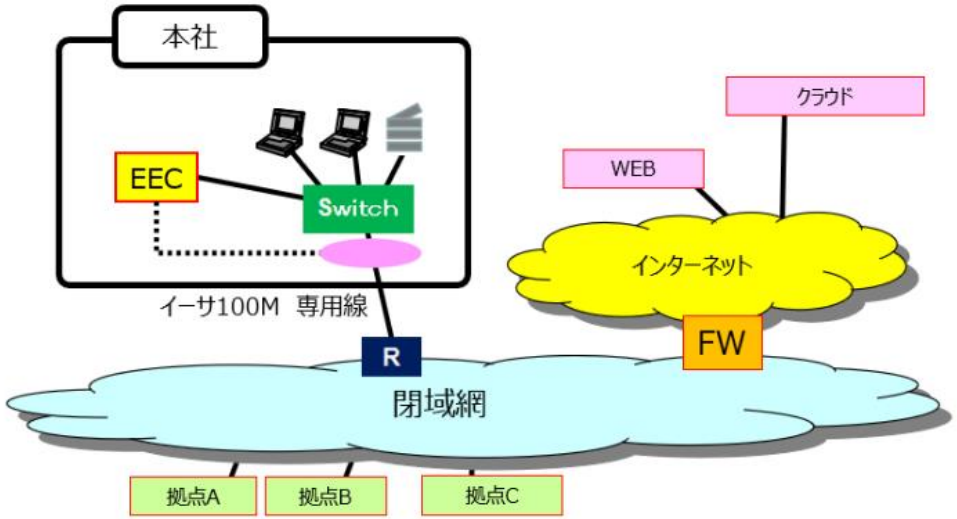
8. パケットキャプチャ Action 例

お客様にオンラインクリニック（Action Report のWEB会議での説明）にて、
お客様より、前ページの **『本社機器a』** の利用者に、アクセス状況を調べたところ 「特殊な通信は行っていない。」
の回答でした。

【事象】
お客様がリアルタイム検索時を利用された際、 頻繁に上位に出てくる端末に気づかれ、詳細を調べました。

2023-07-19 09:58:14 ～ 2023-07-19 10:07:30
【 556 秒 = 9分 16秒 】の約 210万パケットの
発IPのTOPを次に示します。

No	発IP	packet数	%
1	機器A グローバルIP	279526	16.8
2	本社機器 a	254734	15.3
3	本社機器 b	192844	11.6
4	機器B グローバルIP	91657	5.5
5	他拠点機器 a	58851	3.5



この機器の通信は、4529 port でした。
4529 port は、Microsoft Silverlight のアプリで利用する port 番号であることが分かりました。
お客様からの情報では、ネットワークカメラ監視ツール:『Web viewer』が起動していたことが判明しました。
このツールがを常時膨大なパケットを送受信していたと推定されました。

【対応】
Web viewerにアクセスした際、silverlightのインストールを要求されるため、お客様の方で、silverlightをインストールされたと推測されます。
お客様の方では、今後、『Web viewer』を利用されないと言うことで、silverlight についても、アンインストールを実施して頂きました。　以上の対応により、不要なパケットの送信がなくなりました。

9. まとめ

前ページまでの Action をまとめて記述します。

Action_01

○○

Action_02

○○

Action_03

○○

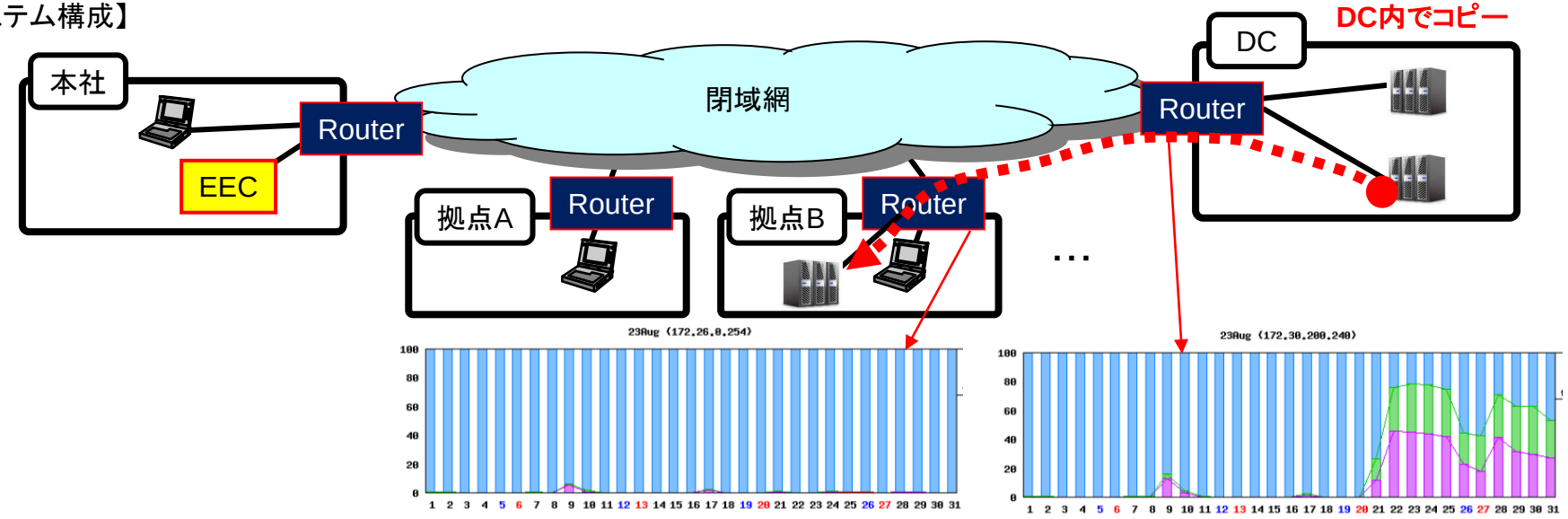
Action ⇒ Monitering ⇒ 検証・Action ⇒　Monitering　を継続することにより、
お客様の　ITインフラサービスの品質を常に向上させていきます。

ITSCのサービスは、「使えば使う程品質が良くなる」をコンセプトに、
常時監視による社内インフラの変化を長期スパンで捉え、社内インフラの品質を
向上させるためのコンサル業務を監視装置と併せて提供する他社には無いサービスです。

10. 他のお客様の事例　（想定外のWAN越えコピー）

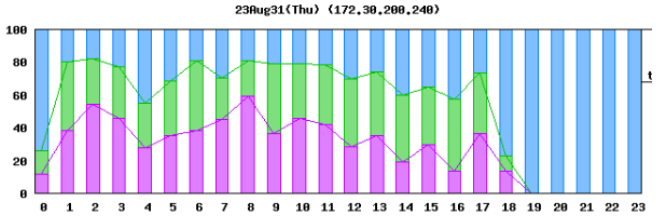
【事象】**8/26にFWの更改を行った。** データが管理画面上に**反映するまで12時間以上かかってしまうこともあり、困っております。**
以前は10分ほどで反映されていました。

【システム構成】



現状は、8/21より、遅延が発生し、業務に影響大。8/21にDC内のコピーを行ったが、既に終了している。

【原因】 調査の結果
お客様は、DC内のコピーは終了していたと考えていましたが、ベンダーが、DCから拠点Bの機器にコピーを行っていたのが判明
コピーを止めることにより、事象は解決した。
お客様は、コピーがされることを把握されていませんでした。



【教訓】
① 想定外の動作があるので、できるだけ見えるかを行う必要がある。
・各拠点のトラフィックの取得、・データセンタにおけるパケットデータの連続取得

② 大量データを出すRouterでは、遅延が発生し、受ける方のRouterでは、遅延が発生しない。
upload は、Routerの負荷が高くなり、遅延となりますので注意が必要です。

遅延が解消 ↑