ITインフラ可視化分析サービスについて

2023年

ITSコンサルティング株式会社

目次

1．会社概要　（http://its-consul.co.jp/）

ITSC ITSコンサルティング株式会社

ＩＴサービスの品質向上を常に続ける
コンサルティングを行います。

ホーム　会社情報　サービス　ITSR [別タグ]　採用情報　お問い合わせ

会社概要

商 号	アイティエスコンサルティング株式会社
設立日	2020年 7月 3日
資本金	300万円
代表取締役社長	山下 亮
所在地	〒160-0022 東京都新宿区新宿1-3-8 YKB新宿御苑ビル3F 316
事業概要	(1) ITサービスに関するコンサルティング (2) ITSR(ITサービスレコーダー）のサービス提供 (3) ITSR(ITサービスレコーダー）の販売 (4) ITサービスに関するシステムのサービス提供 (5) ITサービスに関するシステムの販売 (6) (1)～(5)附帯又は関連する一切の事業

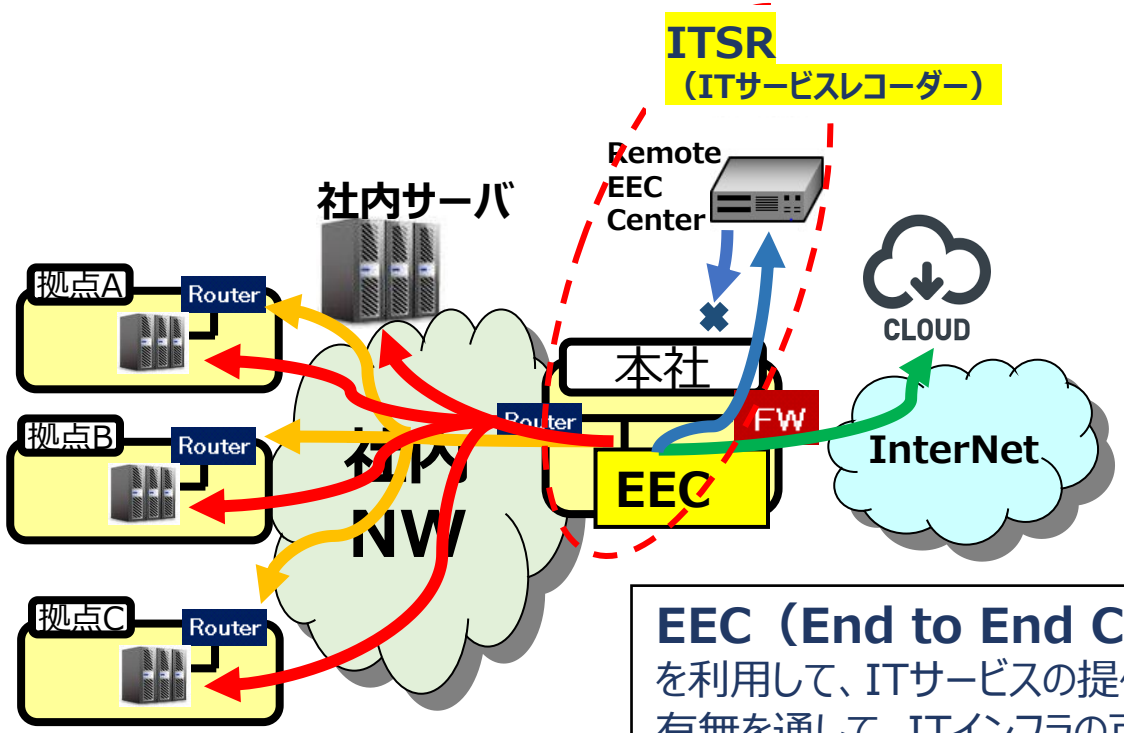
会社情報

- ■ごあいさつ
- ■会社概要
- ■組織図
- ■アクセスマップ
- ■お問い合わせ

2.1 ITインフラ可視化分析サービスとは

ITインフラ可視化分析サービスは、「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。

EECを使用したITSRによる監視サービス ＋ **コンサル業務（アクションレポート）**



EEC（End to End Checker ）
を利用して、ITサービスの提供状況を遅延の有無を通して、ITインフラの可視化を実現。

2.2 ITインフラ可視化分析サービスのサービス内容

サービスには、基本サービスとオプションサービスが有り、オプションサービスはお客様のITインフラ状況に合わせて、必要なサービスをご提供します。

提供形態	サービス名称
基本サービス	**① EECを使用したITSRによる監視サービス**
	・死活試験（ping）
	・ポート試験
	・http、https 試験
	・nameによる試験
	・アラーム表示機能
	・アラーム集計機能
	・Router、サーバのsyslog監視
	② アラーム対応機能
	・アラームシュミレーション機能
	・アラームログ集計機能[Advanced]
	③ アクションレポート
	・アクションレポート
	・オンラインクリニックによるアクションレポート

提供形態	サービス名称
オプションサービス	**④ 追加サービス**
	・パケットキャプチャー
	・４WEB試験
	・突発トラヒックの見える化
	・カスタマイズ試験
	⑤ 付加サービス
	・トラヒック情報の可視化
	・LAN内機器繋がり見える化
	・configの比較
	・運用業務のアウトソーシング

：良く利用されるサービス

2.3 ITインフラ可視化分析サービスの位置づけ

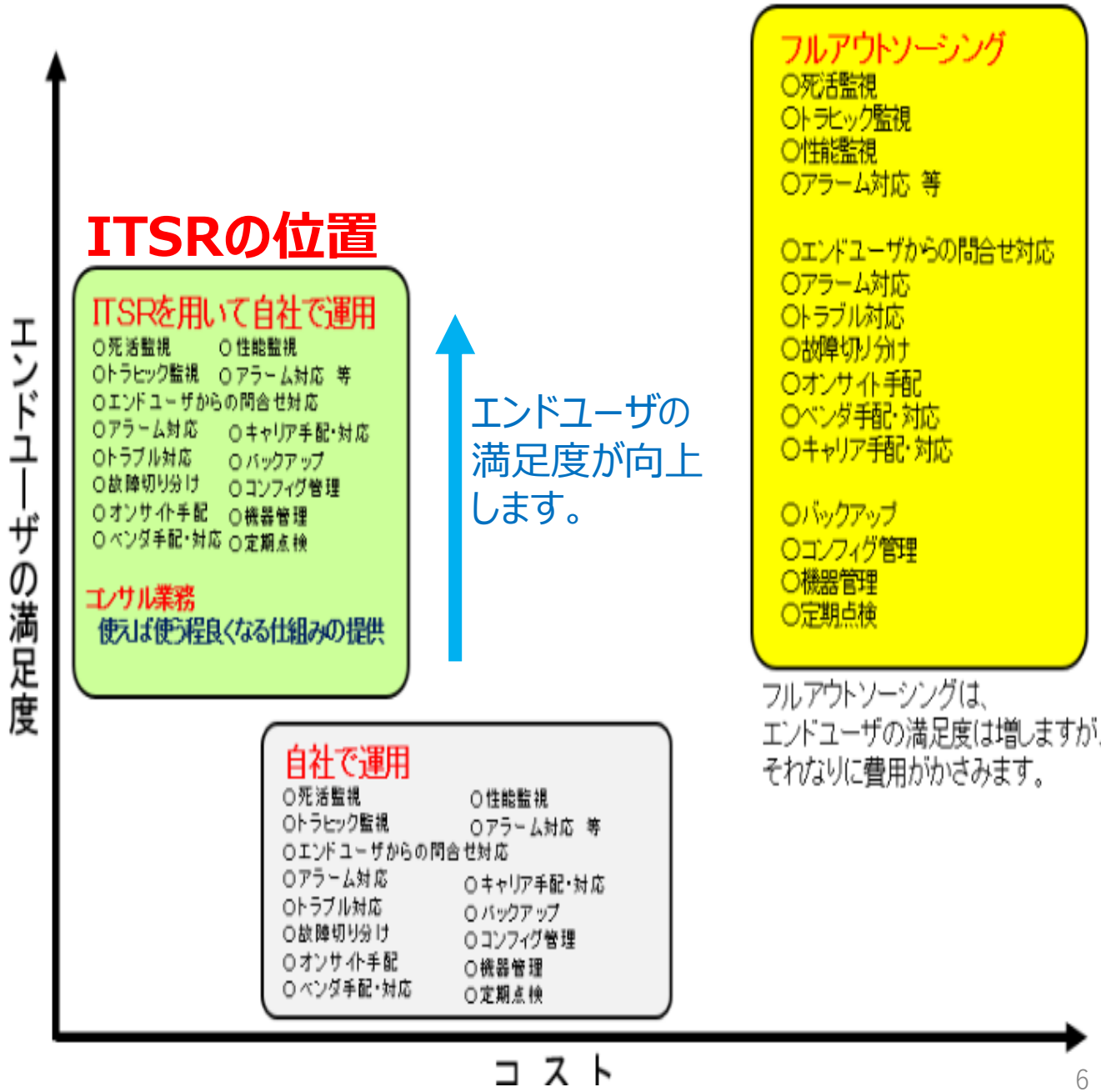
ITインフラ可視化分析サービスのポジショニング

●ITインフラ可視化分析サービスは、
「**使えば使う程品質が良くなる**」をコンセプトに、
監視装置の提供＋コンサル業務で、他社には無い
サービスをご提供します。

提供サービス

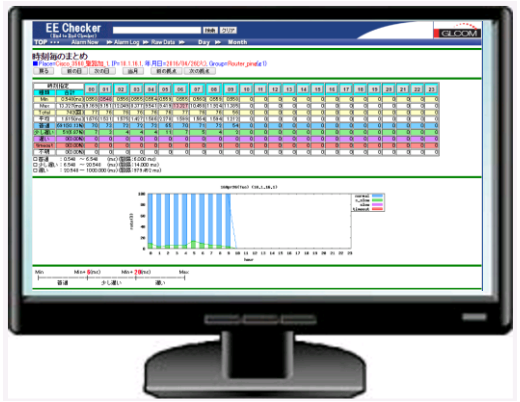
①ITSRの提供(EEC)
②アクションレポート
③オンラインクリニック
④追加サービス

●ITSRを利用することにより監視コストを抑えて、
エンドユーザの満足度を向上できます。

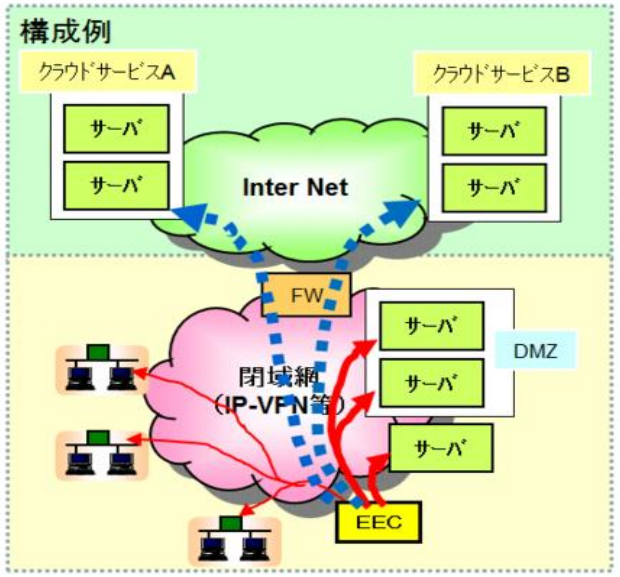


2.4 ITSR（EEC）の設置形態＆可視化

ネットワーク機器、サーバー、クラウド機器の全ての機器をシンプルなワンインタフェースで表示。
（遅延状況を把握）



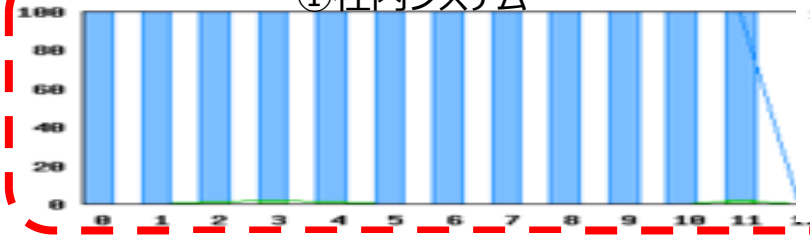
情報システム運用者さま



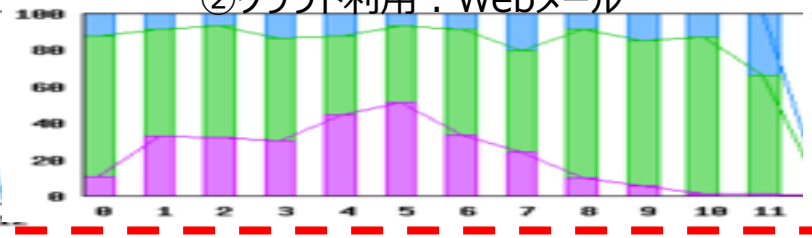
お客さまITインフラへのEEC設置例

＊オンプレミス、クラウドとも同一インターフェースで可視化できます。

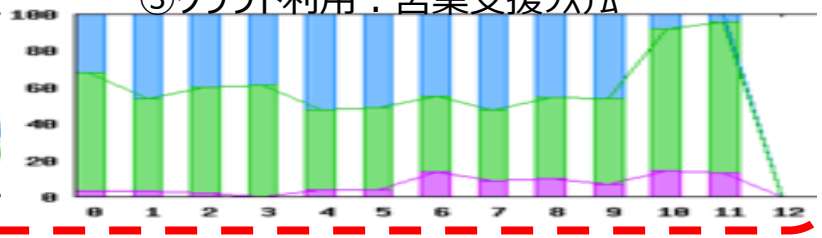
①社内システム



②クラウド利用：Webメール

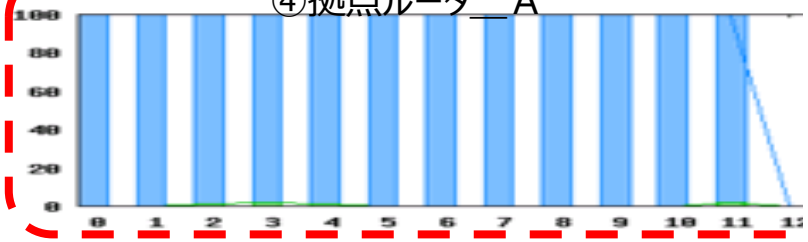


③クラウド利用：営業支援システム

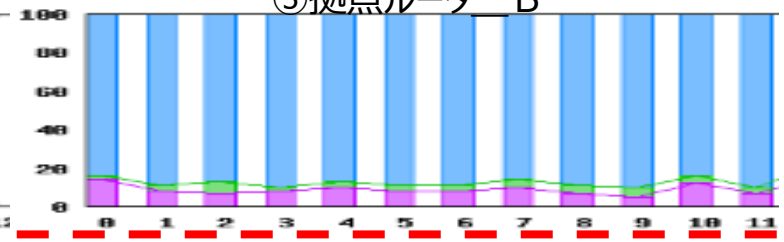


NW機器、FW等

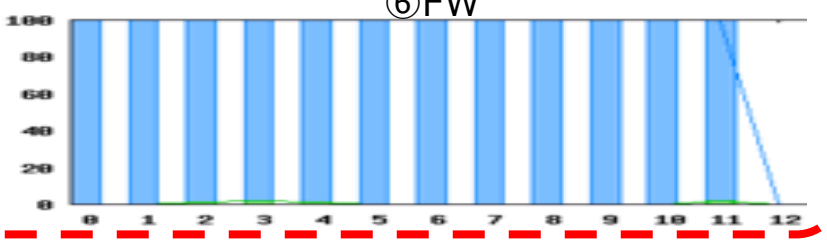
④拠点ルータ＿A



⑤拠点ルータ＿B

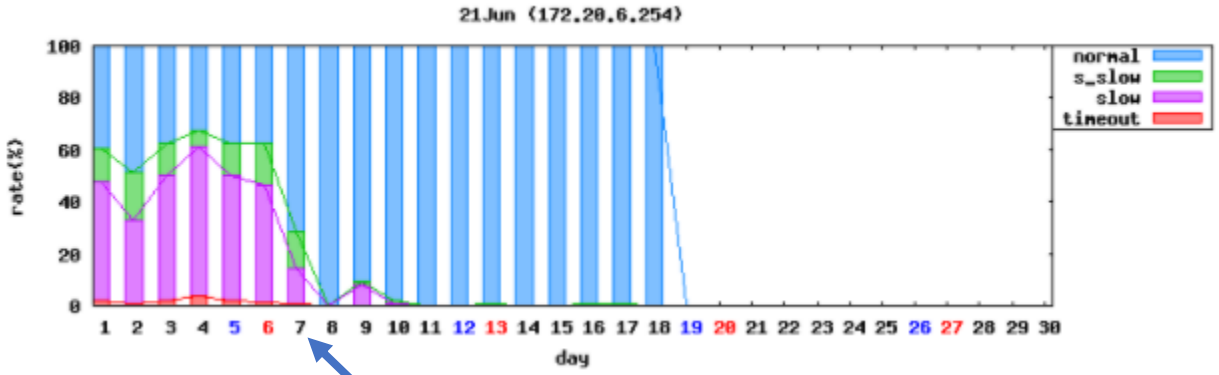


⑥FW



2.5 Ping･Port･https監視によるITインフラの可視化

ITインフラの状況を常時監視する事により、変化をいち早く把握



ネットワーク更改の実施日

平均遅延が大幅に下がった

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
種類	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
Min	3.055(ms)	3.145	3.144	3.100	3.153	3.169	3.092	3.156	3.852	3.829	3.681	4.106	4.113	4.171	4.079	4.099	3.055	4.116	4.125	0	0	0	0	0	0	0	0	0	0	0	0
Max	87.114(ms)	55.164	59.930	66.872	57.553	66.839	87.114	66.517	8.648	50.862	31.720	37.139	10.174	25.773	32.732	10.126	24.251	18.365	6.855	0	0	0	0	0	0	0	0	0	0	0	0
Total	35308(回)	2128	2128	2122	2109	2125	2125	2074	1952	1947	1952	1951	1952	1954	1951	1952	1952	1951	983	0	0	0	0	0	0	0	0	0	0	0	0
平均	11.299(ms)	20.935	16.240	21.301	25.477	22.861	21.534	9.915	4.731	8.143	5.045	5.084	5.008	5.044	5.072	5.057	4.969	5.071	5.067	0	0	0	0	0	0	0	0	0	0	0	0
普通	26725(75.69%)	846	1039	803	696	806	806	1483	1952	1767	1915	1946	1951	1946	1947	1951	1946	1942	983	0	0	0	0	0	0	0	0	0	0	0	0
少し遅い	2013(5.70%)	266	398	261	130	255	331	293	0	20	30	4	1	7	2	1	5	9	0	0	0	0	0	0	0	0	0	0	0	0	0
遅い	6304(17.85%)	970	675	1017	1201	1025	957	289	0	158	7	1	0	1	2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
timeout	266(0.75%)	46	16	41	82	39	31	9	0	2	0	0	0	0	0	0	0	0	0	0	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	0	0	0	0	0	0

□普通　：3.055 ～9.055　(ms) (間隔：6.000 ms)
□少し遅い：9.055 ～23.055　(ms) (間隔：14.000 ms)
□遅い　：23.055～1000.000 (ms) (間隔：976.945 ms)

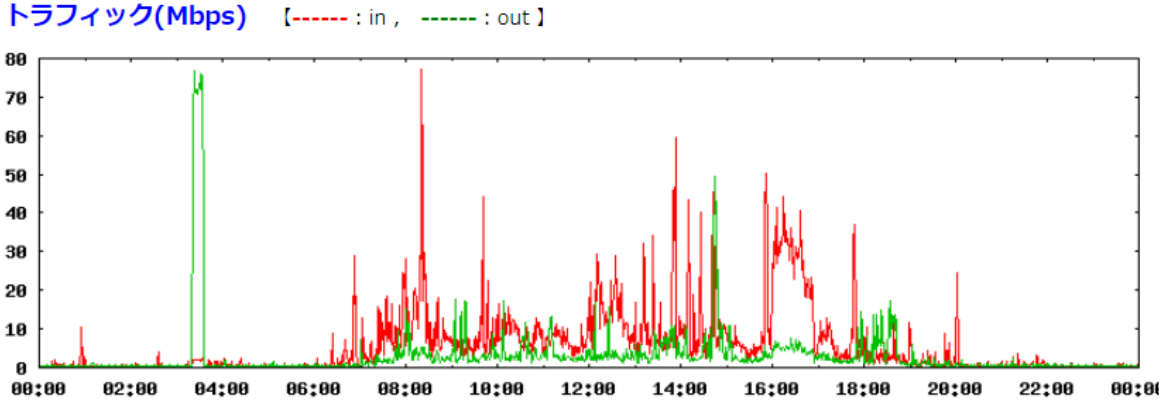
毎日、timeoutが多く発生していたが
ネットワーク更改後は、ほぼ無くなった

2.6 SNMPを利用したITインフラの可視化

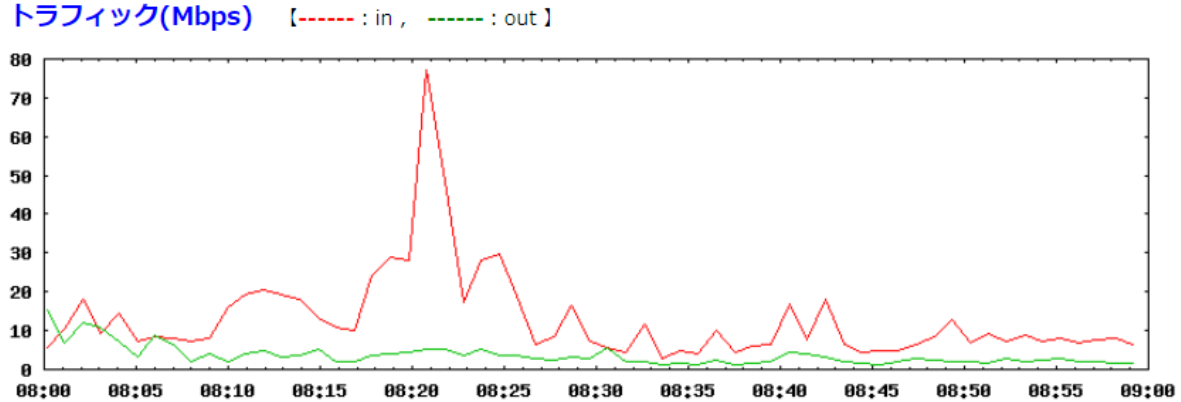
Ping監視＋SNMP（トラヒック情報）によるITインフラの可視化

HUB、RouterからSNMP情報を取得する事により、トラヒック情報の可視化を実現

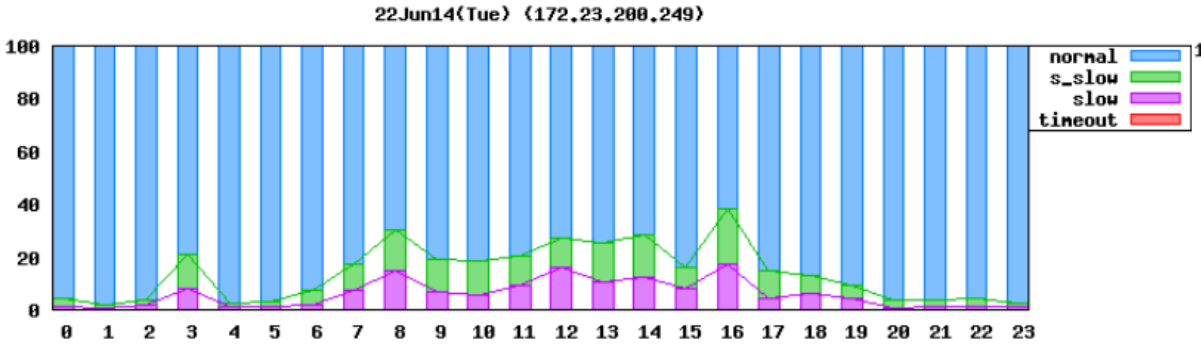
終日のトラヒック状況



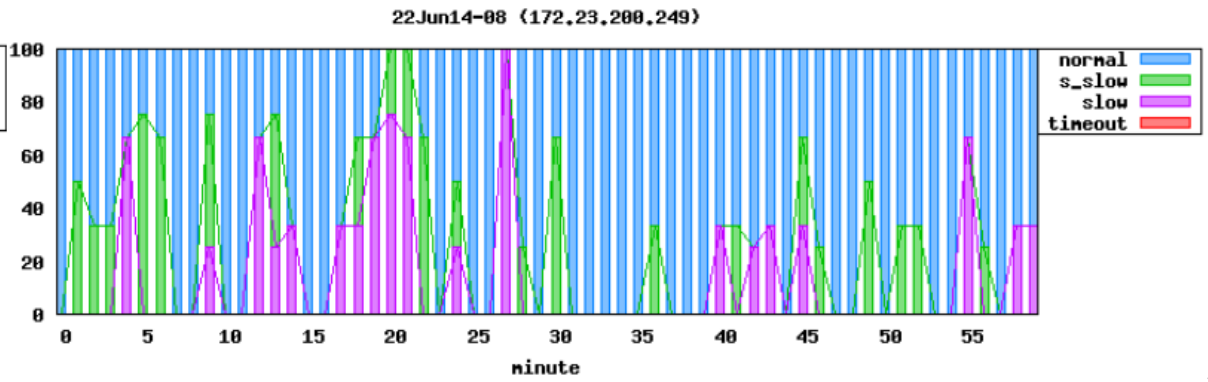
８時台のトラヒック状況



終日のPing状況



８時台のPing状況



2.7 パケットキャプチャーによるネットワーク分析の容易化

1000万パケットの分析が可能（誰が何処へ接続して、何の通信を行っていたかが容易に判ります）

【logファイル一覧】　SnapShotデータの検索

◇ 元となる cap ファイルを指定して下さい。例：renzoku_5_230110_102002.cap

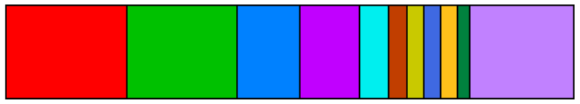
renzoku_5_230214_121802.cap ←log fileを選択 または、 renzoku_0_230214_121802.cap log file名を直接入力して下さい。

↑直接入力の方が優先されます。

元となる cap ファイル： **renzoku_0_230214_121802.cap**
開始～終了 capファイル： **0 ～ 5**　【ファイル数：6　約 60 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：2023-02-14 11:28:59 ～ 2023-02-14 12:18:02 【 2943 秒 = 49 分 3 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	10.0.1.12	113209	23.7	
2	74.125.250.157	72574	15.2	google
3	10.0.1.14	51888	10.9	
4	10.0.1.16	42348	8.9	
5	224.63.110	30166	6.3	
6	94.254.151	20114	4.2	
7	173.194.51.6	15218	3.2	google
8	172.217.175.14	12396	2.6	google

No	着IP	packet数	%
1	10.0.1.12	128091	26.9
2	74.125.250.157	94663	19.9
3	10.0.1.14	70847	14.9
4	10.0.1.16	43703	9.2
5	242.130.174	16256	3.4
6	94.254.151	15493	3.3
7	172.217.175.238	9979	2.1
8	10.0.1.10	6959	1.5

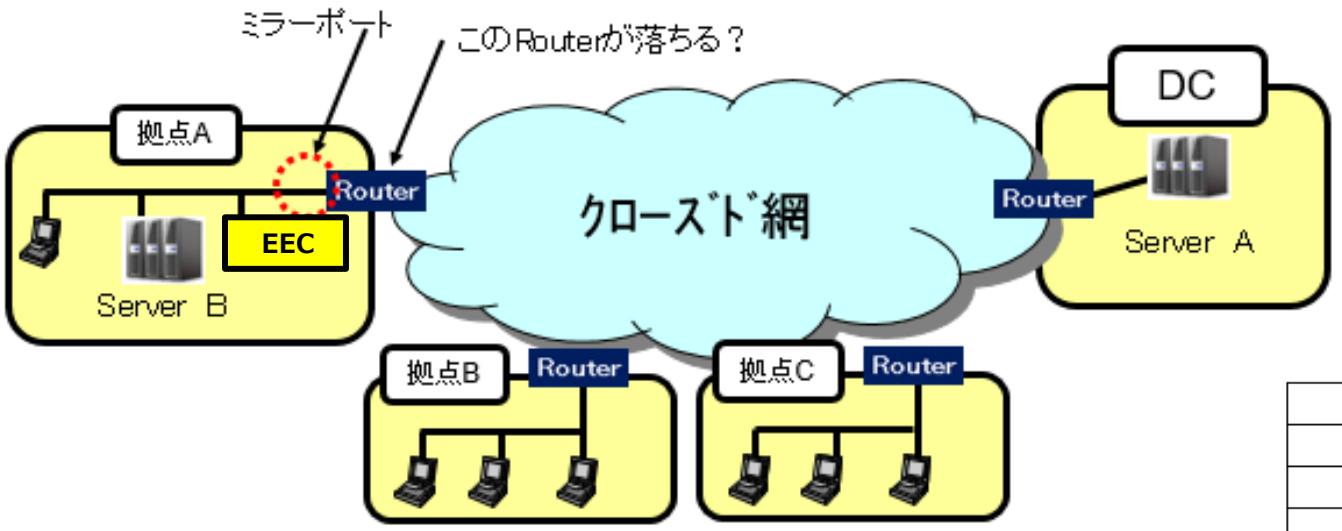
No	発プロトコル	packet数	%
1	https	143035	32.5
2	stun	72531	16.5
3		46421	10.5
4	52950	31215	7.1
5	52750	27175	6.2
6	microsoft-ds	17162	3.9
7	63193	14757	3.4
8	51172	11732	2.7

No	着プロトコル	packet数	%
1	stun	94620	21.3
2	https	85793	19.3
3	52950	48838	11.0
4		46421	10.5
5	60988	22656	5.1
6	52881	15218	3.4
7	http	13524	3.0
8	51833	13366	3.0

ITインフラ可視化分析サービスによる
原因の発見事例のご紹介

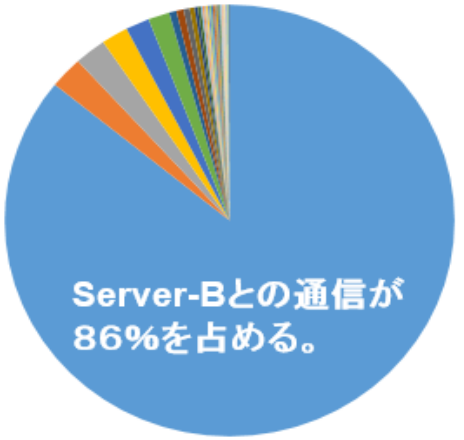
3.1 パケットキャプチャーによる問題解決例①

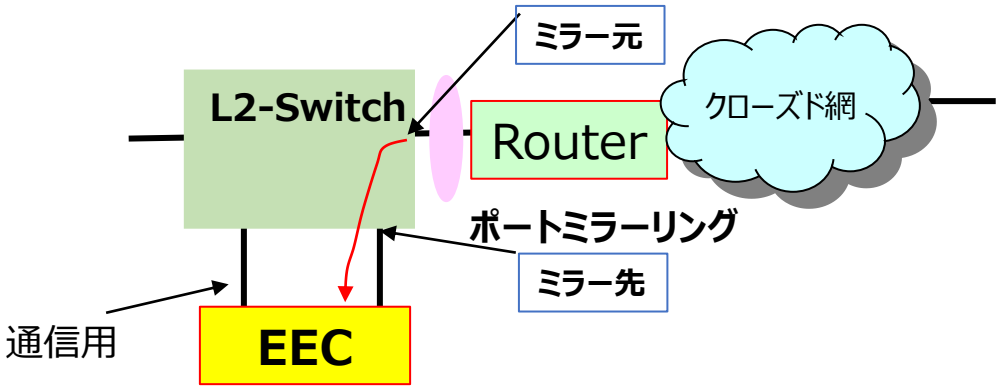
DC（Data Center）にあるServer-Aとの通信が遅い



パケットキャプチャーによる
新たに発見されたサーバーの通信

	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





- **Server-Bの通信が影響することが判明**
- Server-Bがどの拠点の機器と通信を行っているか調べたところ、そのほとんどが、拠点B,C,D, …. との通信。

3.2 パケットキャプチャーによる問題解決例②

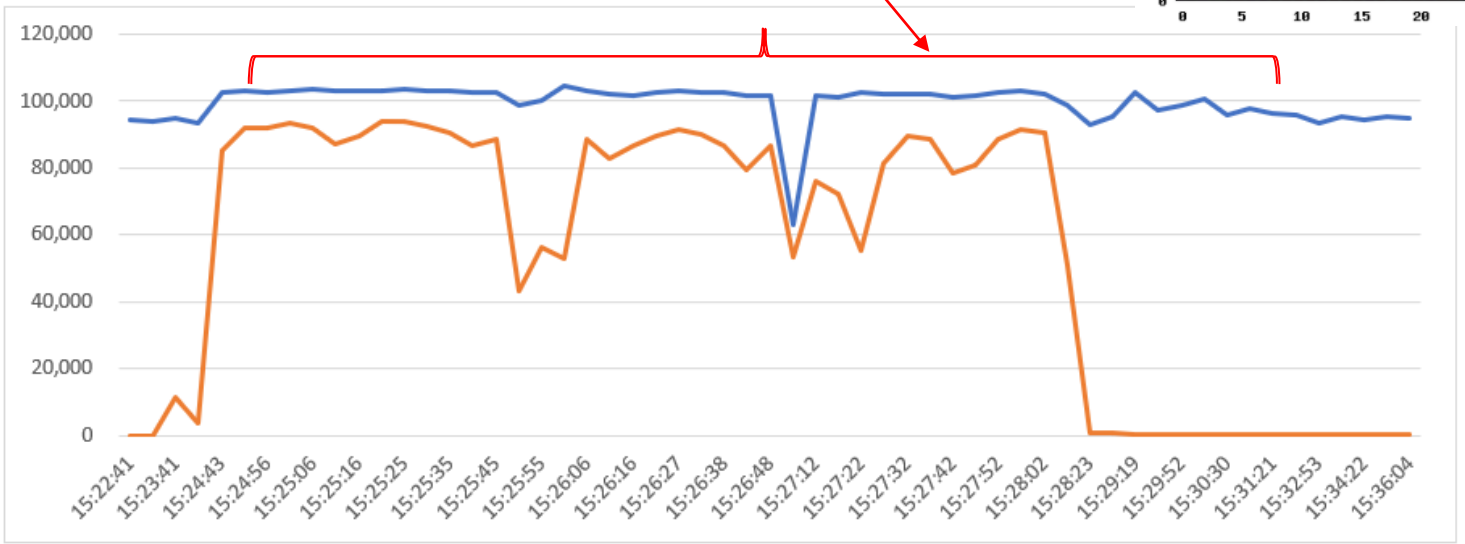
Web会議中に音声が途切れる

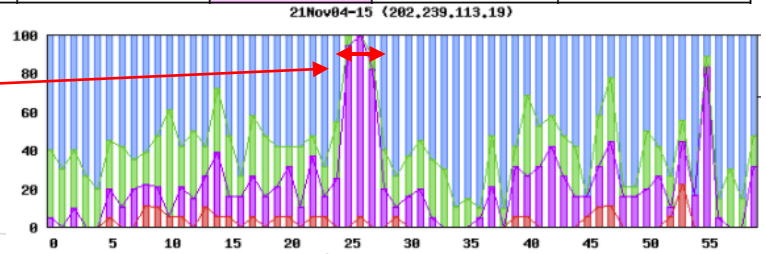
192.168.50.101 の通信について

No	新ファイル名	試験時間 開始	~	終了	時刻差	全パケット パケット数	length (byte)	length累計 (byte)	192.168.50.101 パケット数	length (byte)	length累計 (byte)
1	B_P_211104_2.cap	15:22:41	~	15:23:09	0:00:28	94,457	64,540,420	64,540,420	2	92	92
2	B_P_211104_2.cap1	15:23:09	~	15:23:41	0:00:32	93,982	53,205,056	117,745,476	2	92	184
3	B_P_211104_2.cap2	15:23:41	~	15:24:10	0:00:29	94,641	56,532,646	174,278,122	11,286	9,529,145	9,529,329
4	B_P_211104_2.cap3	15:24:10	~	15:24:43	0:00:33	93,462	66,345,059	240,623,181	3,710	1,670,811	11,200,140
5	B_P_211104_2.cap4	15:24:43	~	15:24:50	0:00:07	102,284	74,217,939	314,841,120	85,276	63,287,356	74,487,496
6	B_P_211104_2.cap5	15:24:50	~	15:24:56	0:00:05	102,981	75,537,702	390,378,822	91,931	68,844,554	143,332,050

遅延と対応

この機器で、パケットを占有





15時代

3.2 パケットキャプチャーによる問題解決例③

パケット分析による原因の特定化

15:22:41 ～ 15:25:20 のデータ（logファイル最初から 12file分）をWireSharkで表示してみます。
192.168.50.101　の通信　パケット

紫色が多くなっています。 MS-RPCプロトコル

お客様自身で検索できる機能も有しています。

ip.addr==192.168.50.101

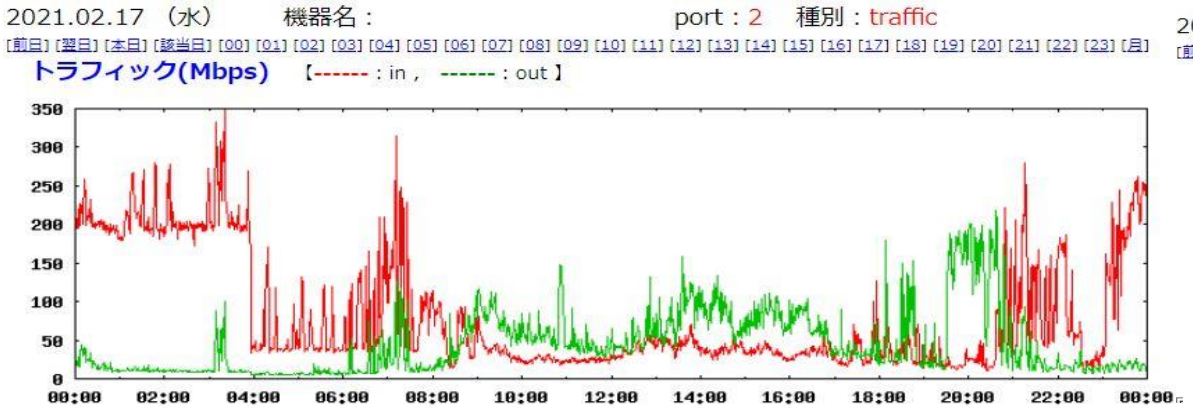
No.	Time	Source	Destination	Protocol	Length	Info
220371	15:23:51.171046	192.168.200.11	192.168.50.101	KRB5	267	KRB-ERROR[Packet size limited during capture]
220372	15:23:51.171317	192.168.50.101	192.168.200.11	TCP	64	58371 → 88 [FIN, ACK] Seq=228 Ack=214 Win=262656 Len=0
220373	15:23:51.171781	192.168.50.101	192.168.200.11	TCP	70	58372 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
220374	15:23:51.172234	192.168.200.11	192.168.50.101	TCP	60	88 → 58370 [ACK] Seq=1552 Ack=1534 Win=65536 Len=0
220375	15:23:51.172242	192.168.200.11	192.168.50.101	TCP	60	88 → 58370 [RST, ACK] Seq=1552 Ack=1534 Win=0 Len=0
220376	15:23:51.172684	192.168.200.10	192.168.50.101	TCP	60	49155 → 58365 [ACK] Seq=1 Ack=1878 Win=65536 Len=0
220377	15:23:51.172689	192.168.200.10	192.168.50.101	DCERPC	339	Bind_ack: call_id: 2, Fragment: Single[Packet size limited during capture]
220379	15:23:51.173199	192.168.50.101	192.168.200.10	DCERPC	278	Alter_context: call_id: 2, Fragment: Single[Packet size limited during capture]
220392	15:23:51.177259	192.168.200.11	192.168.50.101	TCP	60	88 → 58371 [ACK] Seq=214 Ack=229 Win=65536 Len=0
220393	15:23:51.177323	192.168.200.10	192.168.50.101	DCERPC	159	Alter_context_resp: call_id: 2, Fragment: Single[Packet size limited during capt
220394	15:23:51.177326	192.168.200.11	192.168.50.101	TCP	60	88 → 58371 [RST, ACK] Seq=214 Ack=229 Win=0 Len=0
220395	15:23:51.178087	192.168.200.11	192.168.50.101	TCP	66	88 → 58372 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1240 WS=256 SACK_PERM=1
220396	15:23:51.178375	192.168.50.101	192.168.200.11	TCP	64	58372 → 88 [ACK] Seq=1 Ack=1 Win=262656 Len=0
220397	15:23:51.178613	192.168.50.101	192.168.200.11	KRB5	365	AS-REQ[Packet size limited during capture]
220398	15:23:51.181214	192.168.50.101	192.168.200.10	DCERPC	326	Request: call_id: 2, Fragment: Single[Packet size limited during capture]
220399	15:23:51.185562	192.168.200.10	192.168.50.101	DCERPC	258	Response: call_id: 2, Fragment: Single[Packet size limited during capture]
220400	15:23:51.185668	192.168.200.11	192.168.50.101	KRB5	1523	AS-REP[Packet size limited during capture]
220401	15:23:51.185940	192.168.50.101	192.168.200.11	TCP	64	58372 → 88 [FIN, ACK] Seq=308 Ack=1470 Win=262656 Len=0
220402	15:23:51.186408	192.168.50.101	192.168.200.10	DCERPC	294	Request: call_id: 3, Fragment: Single[Packet size limited during capture]
220403	15:23:51.186416	192.168.50.101	192.168.200.11	TCP	70	58373 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
220414	15:23:51.191919	192.168.200.10	192.168.50.101	DCERPC	402	Response: call_id: 3, Fragment: Single[Packet size limited during capture]
220415	15:23:51.192425	192.168.50.101	192.168.200.10	DCERPC	198	Request: call_id: 4, Fragment: Single[Packet size limited during capture]
220416	15:23:51.192433	192.168.200.11	192.168.50.101	TCP	60	88 → 58372 [ACK] Seq=1470 Ack=309 Win=65536 Len=0
220418	15:23:51.193027	192.168.200.11	192.168.50.101	TCP	60	88 → 58372 [RST, ACK] Seq=1470 Ack=309 Win=0 Len=0
220419	15:23:51.193036	192.168.200.11	192.168.50.101	TCP	66	88 → 58373 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1240 WS=256 SACK_PERM=1

3.4 トラヒック情報の可視化による原因の特定化例①

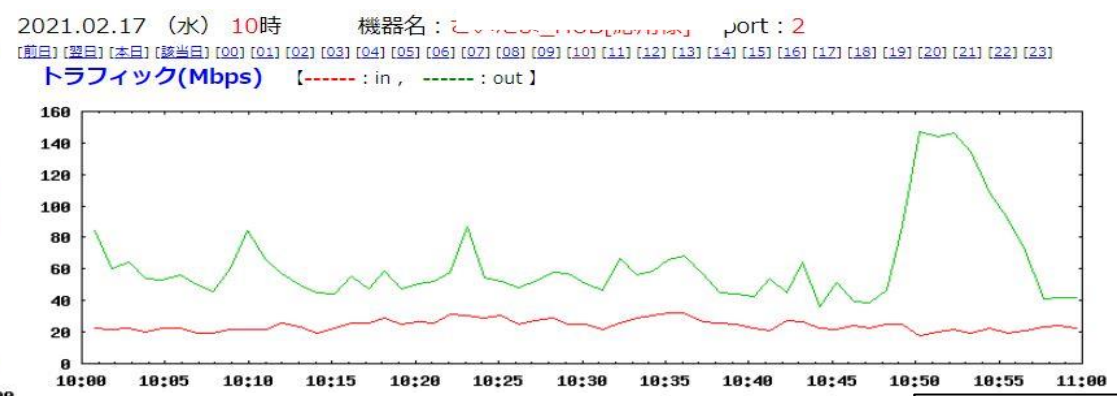
Ping監視でtimeoutが発生しているがトラヒックは少ない

・各機器（Router、Switch等）のsnmp情報を継続的に入手し、そのデータの可視化
・可視化したトラヒック情報と、Ping監視情報を合わせる事により、原因の特定化を実施
（ネットワークキャリアでの公平制御による帯域制限でした）

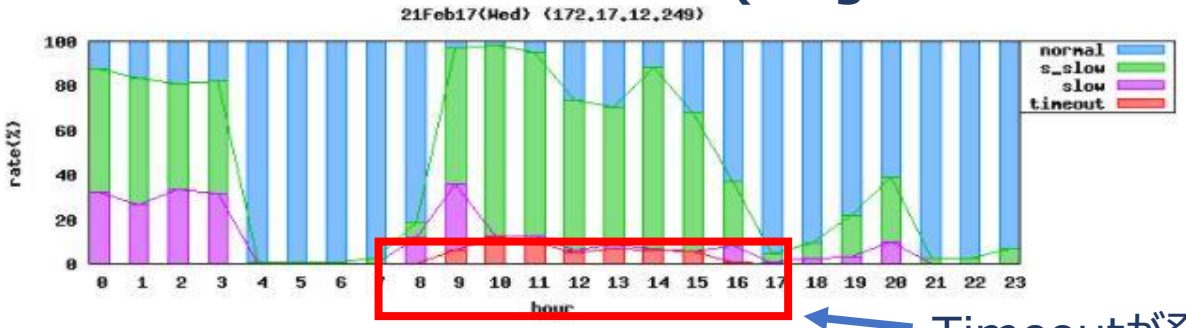
終日のトラヒック状況



10時台のトラヒック状況

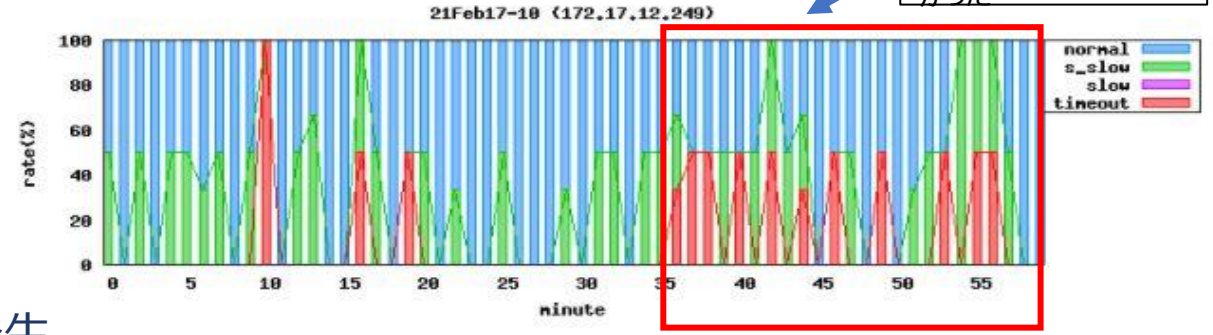


終日の遅延状況(Pingで監視)



Timeoutが発生

10時台の遅延状況

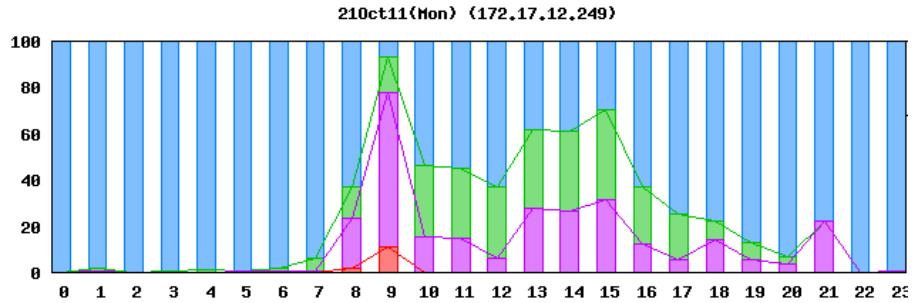


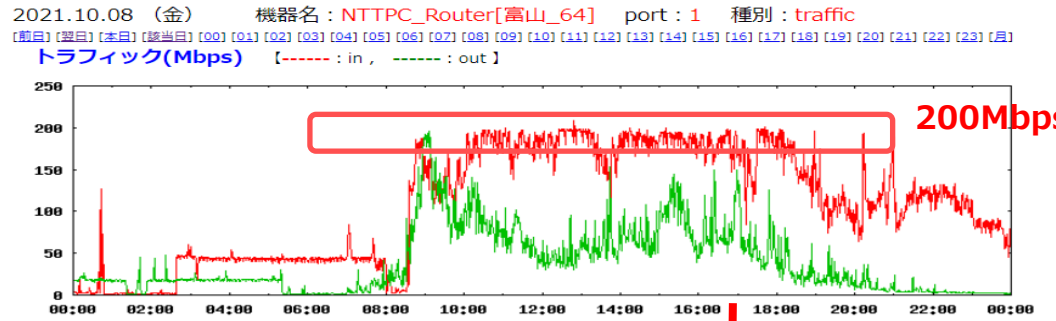
特に、10時35分～56分までが使いづらかった

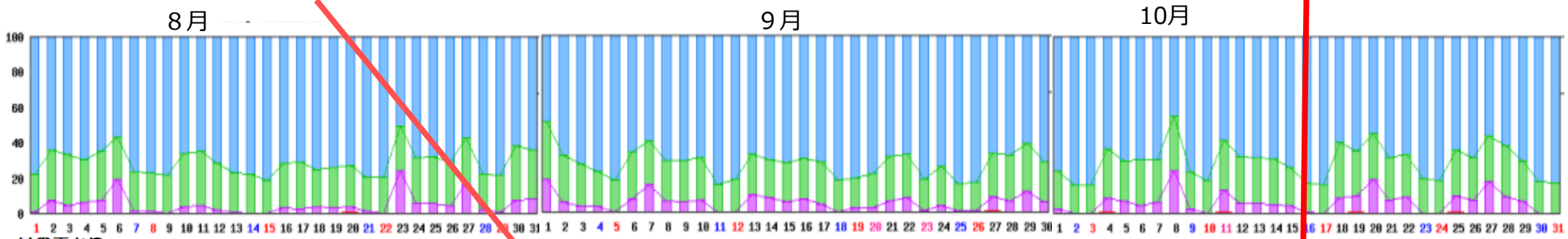
3.5 トラヒック情報の可視化による原因の特定化例②

専用線ネットワークが遅い

お客様のエンドユーザ様からネットワークが遅いとの申告が情報システム部にあり、Ping監視状況を見ると毎週月曜日の9時台はtimeoutが多く発生。
トラヒック情報により、9時台のinのトラヒックが頭打ちになっていることを確認し、専用線を200Mbpsから300Mbpsへ増速。







月のまとめ

■ Place=情報システム事業部, IP=172.22.50.254, 年月=2021/10, Group=ping試験_東(g4)

戻る　前の月　次の月　前の拠点　次の拠点

10月

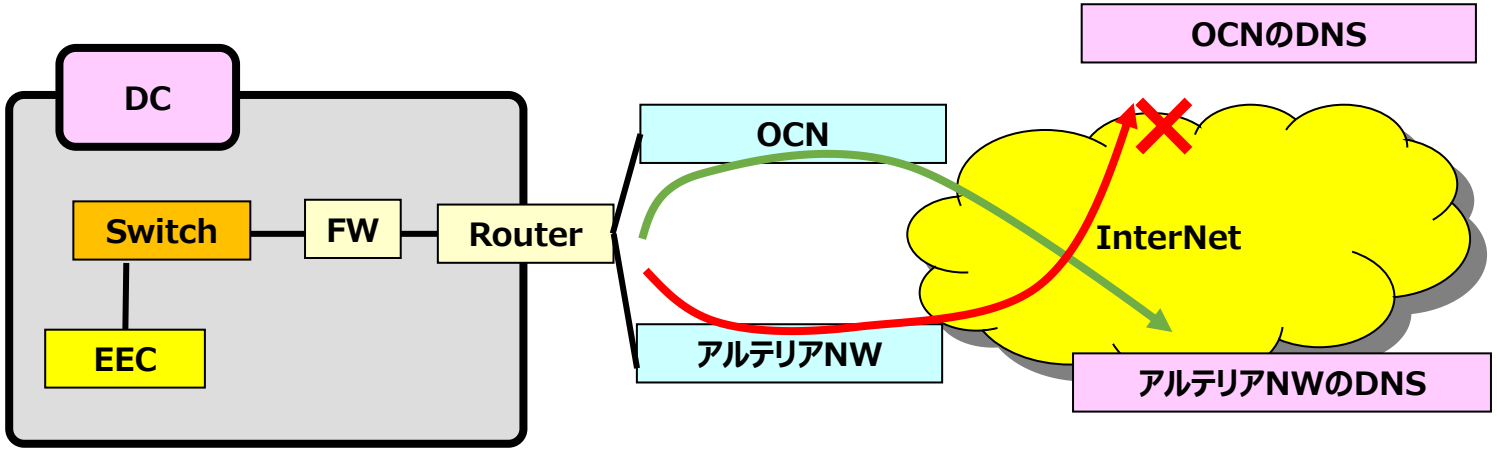
日の指定		01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
種類	合計	金	土	日	月	火	水	木	金	土	日	月	火	水	木	金	土	日	月	火	水	木	金	土	日	月	火	水	木	金	土	日
Min	16.186(ms)	16.366	16.333	16.335	16.325	16.328	16.337	16.359	16.278	16.346	16.308	16.340	16.303	16.316	16.341	16.285	16.356	16.374	16.291	16.223	16.353	16.218	16.328	16.336	16.350	16.349	16.311	16.200	16.294	16.186	16.376	16.301
Max	112.611(ms)	46.420	41.475	25.861	86.652	112.611	47.871	72.351	55.656	33.790	43.947	108.489	77.211	70.704	49.123	59.617	43.013	41.878	58.402	89.370	65.886	65.571	77.978	39.186	36.168	63.742	47.837	57.617	56.635	59.175	44.483	45.768
Total	96055(回)	3107	3109	3109	3092	3094	3100	3100	3096	3107	3107	3090	3103	3101	3104	3101	3104	3101	3094	3080	3090	3097	3093	3102	3099	3089	3097	3091	3094	3097	3103	3104
平均	17.864(ms)	17.322	16.994	16.971	18.268	18.113	17.604	17.987	20.499	17.285	16.986	18.917	17.738	17.815	17.719	17.568	17.033	16.965	18.131	18.429	19.240	17.978	18.313	17.018	16.986	18.406	17.960	19.536	18.219	17.856	17.003	16.980
普通	67810(70.59%)	2367	2608	2613	1970	2171	2153	2171	1402	2375	2528	1643	2102	2126	2153	2302	2570	2598	1845	2005	1695	2121	2055	2489	2529	1979	2122	1741	1905	2187	2551	2564
少し遅い	22244(23.16%)	664	494	492	861	706	817	744	956	649	578	872	831	803	802	669	515	501	990	780	804	751	756	605	567	801	740	796	901	705	546	537
遅い	5870(6.11%)	76	7	4	245	208	124	181	737	83	1	384	169	171	148	128	19	1	250	282	585	225	275	8	3	287	230	549	280	200	6	3
timeout	131(0.14%)	0	0	0	16	9	6	4	1	0	0	16	1	1	1	2	0	0	9	13	6	0	7	0	0	16	5	5	8	5	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	0	0	0	0	0	0	0

3.6 インターネット接続、時々接続不可の解決例

インターネット接続を行うと、繋がる時と繋がらない時が有る（1年間、原因が解らず利用）

NTTPC社HPへの https試験結果

```
00:00:16 : 162.295
00:00:54 : 172.336
00:01:34 : 154.492
00:02:12 : timeout
00:02:52 : timeout+2
00:03:32 : 164.122
00:04:09 : 167.506
00:04:47 : 145.995
00:05:24 : 162.548
00:06:02 : 158.809
00:06:39 : 148.105
00:07:16 : timeout
00:07:57 : timeout+2
00:08:37 : 169.138
00:09:14 : 163.730
00:09:52 : 166.113
00:10:29 : 136.558
00:11:06 : 160.879
00:11:44 : 159.195
00:12:21 : timeout
00:13:02 : timeout+2
00:13:42 : 168.205
00:14:19 : 164.535
00:14:57 : 158.140
00:15:34 : 160.438
00:16:11 : 177.221
00:16:52 : 165.423
00:17:29 : timeout
00:18:09 : timeout+2
00:18:50 : 169.077
00:19:27 : 167.418
```



５分毎ぐらいに
Timeout が２回連続しています。

非常に規則的に timeout が生じています。

調査結果：お客様サポートのSE会社がOCNの仕様を見過ごしていた。

◇ 複数のISPをご利用の場合のDNSの設定に関する注意点
DNSサーバーのセキュリティ制限実施のお知らせ
https://www.ocn.ne.jp/business/info/130930.html より

抜粋　OCN以外のISP回線契約上で、上記対象DNSサーバーで名前解決を行う設定をされていた場合、インターネットへの接続が不可となります

3.7 ITインフラ可視化分析サービスによる原因の発見事例

ITSC

改善を図った実績

FW、Proxy、Routerに起因すること

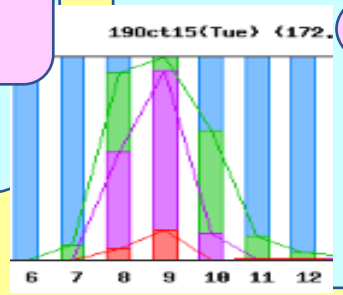
office365の遅延
⇒**「office365遅延の原因の究明手順」を策定**

Routerにて、ﾌﾟﾛｾｽがある時間保持のため遅延が発生

他の機器に起因すること

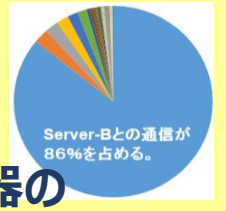
他機器の影響
WidowsUP関連

←帯域に余裕があるのにRouterが落ちる
↓
あるサーバーが異常ﾊﾟｹｯﾄを大量送信



ﾍﾞｽﾄｴﾌｫｰﾄで
timeoutが頻発

←遅延は少ないが、
timeoutが目立つ



問題のある機器のIPを発見して解決

帯域に関すること

お客様要望
「帯域不足は理解できたが、どの様なパケットで、不要なパケットが無い事を証明できないと、増速の決裁が取れない」
遠隔でﾊﾟｹｯﾄｷｬﾌﾟﾁｬｰを実施し、分析。
お客様は納得して、増速に至る。

ｷﾞｬﾗﾝﾃｨ回線（UNO)しかﾄﾗﾌｨｯｸﾚﾎﾟｰﾄがﾞ出せない。
⇒**SNMP-Graphで実現**

遅延と帯域不足は
相関性有り
⇒ **見える化の実現**

DNSに起因すること

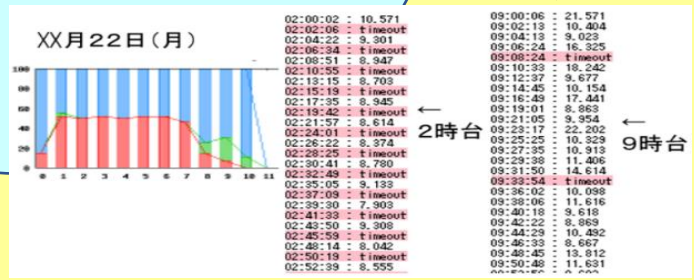
SalesForce
の遅延例

Office36
5の遅延例

古いDNSが登録されていた

ﾄﾗﾌｨｯｸが多くなった方が若干改善された
↓

↑
冗長化の一台が不適切な設定



4. 最後に

ITインフラ可視化分析サービスの基本サービス

① 常時監視サービス（EECの貸出）

・監視したいネットワーク機器、サーバをＥＥＣに登録し、常時監視サービスを提供します。
・アラートが発生した場合には、メールにて、お客さまに通知されます。

② アクションレポートサービス

・アクションレポートは、ＩＴサービスの品質を向上させていくためには大変重要です。
・エンドユーザさまからの申告の前に、ＩＴインフラの不具合を発見し改善を続けるため、
３カ月に１回、アクションレポートをお客さまに提出します。

③ オンラインクリニックサービス

・３カ月に１度のペースで、電話会議または、ビデオカンファレンスにより、アクションレポートのご説明を行います。
・ＩＴインフラサービスの安定した提供のため、アクションを計画し品質を更に向上させます。
・特に問題が無いときでも、閾値を見直し、悪いもの（拠点、機器）の５％を常に改善するようにします。

①～③を繰り返すことにより、良いデータと悪いデータを比較し、問題個所をあぶり出します。

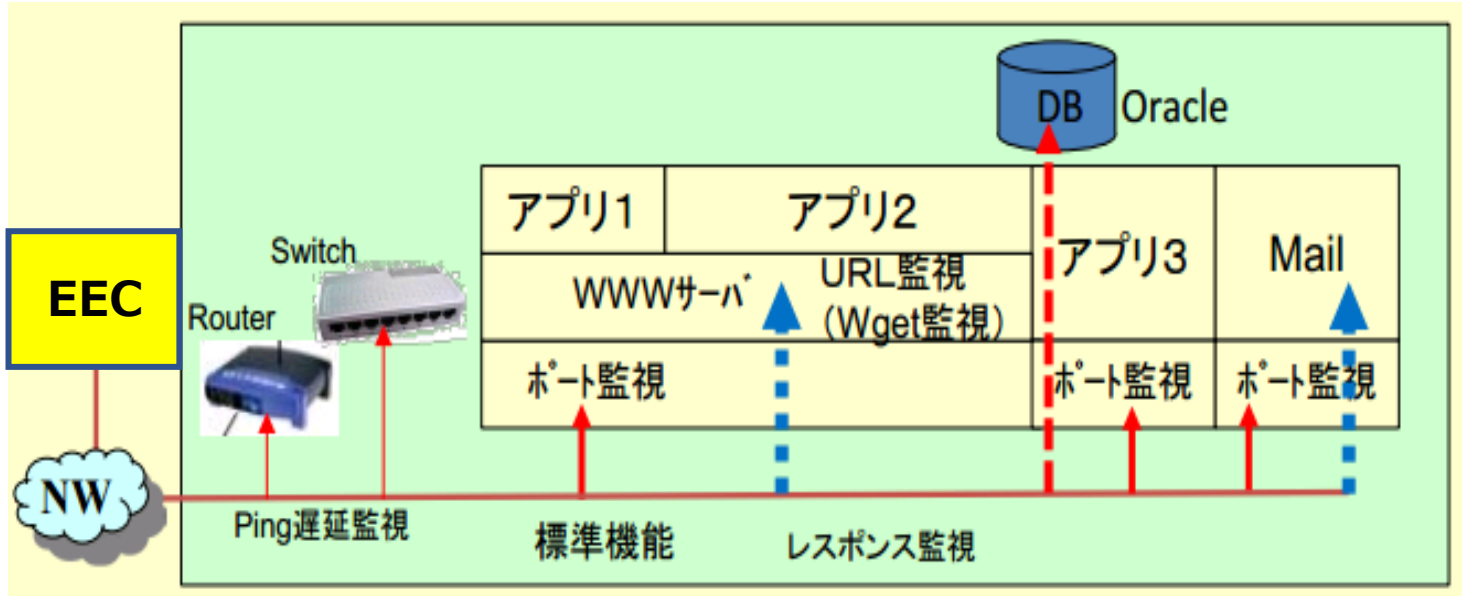
ITインフラ可視化分析サービスは、
ITインフラの品質を常に向上させる仕組みを提供します。

参考1. 保守・運用サービスに必要なポイント（ポイント１）

アプリケーションレイヤに近いレベルからの試験の有効性

サーバのCPU能率、メモリ使用量、コネクション数、使用可能ディスク容量、死活監視では、**お客さまの真のお困りが分かりません。**

ITSRにより、よりアプリに近い試験を行うことにより困り具合を見える化



ping監視、ポート監視より上位の、**サービス監視（URL監視）**を行い
且つ、応答のレスポンスを常時把握することにより、**お客さまのストレス（体感）を見える化**します。

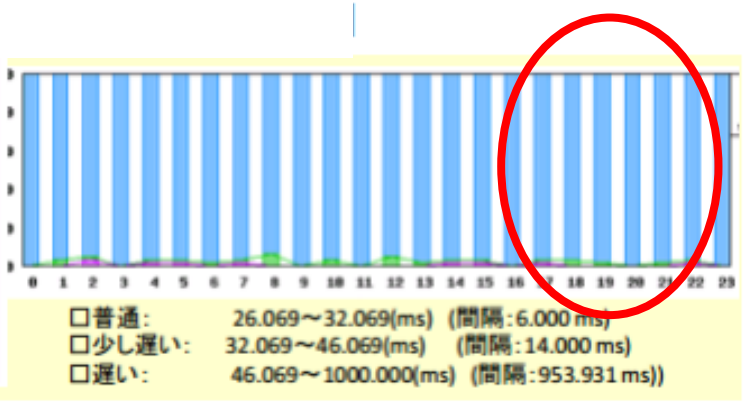
参考1.1 アプリケーションレイヤに近いレベルからの試験の有効性

ポート監視では異常が発見できない場合でも、よりアプリに近いURL監視（http/https）試験を実施すると実際にWebサーバの情報を取得するので、お客様が感じたストレス状況を把握する事ができます。

（http/https試験は、０バイトの情報を入手するオプションコマンドで実施します）

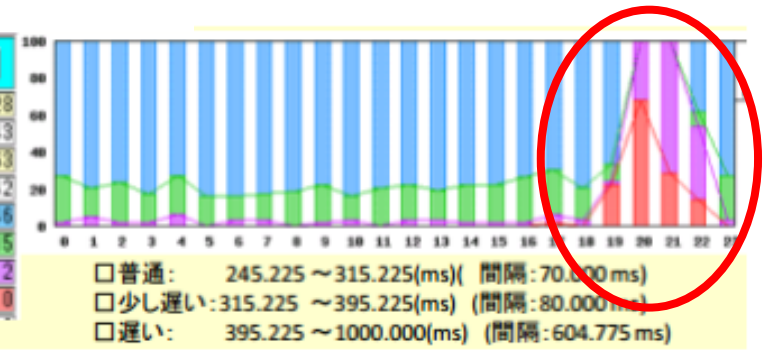
ポート監視の例

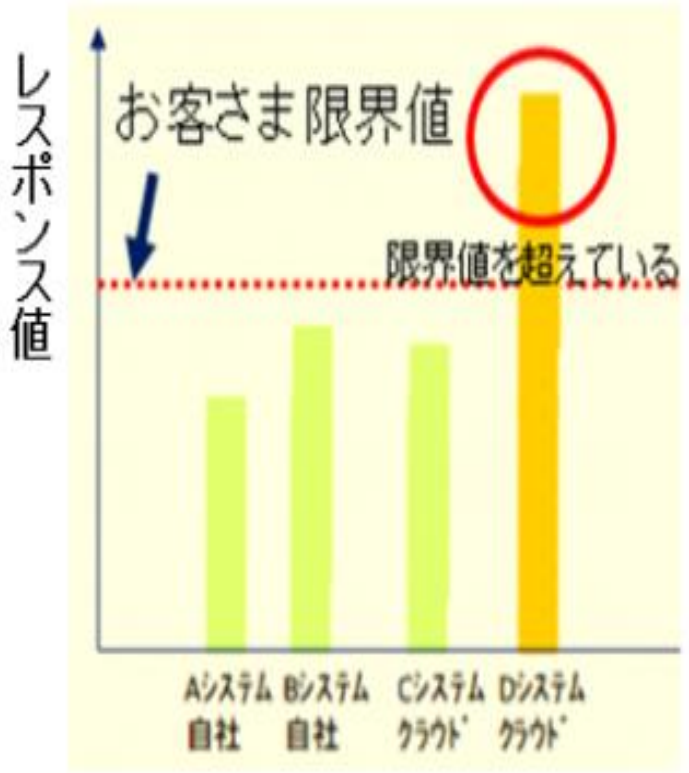
時刻指定		17	18	19	20	21	22	23
種類	合計							
Min	26.069(ms)	26.123	26.275	26.207	26.254	26.300	26.272	26.150
Max	247.444(ms)	76.483	34.016	36.187	30.282	44.380	59.070	29.612
Total	1507(回)	62	63	63	63	62	63	63
平均	28.730(ms)	29.168	28.469	28.441	27.868	28.405	28.938	27.994
普通	1473(97.74%)	60	61	62	63	61	61	63
少し遅い	25(1.66%)	1	2	1	0	1	1	0
遅い	9(0.60%)	1	0	0	0	0	1	0
timeout	0(0.00%)	0	0	0	0	0	0	0



URL監視（http/https）の試験結果

時刻指定		17	18	19	20	21	22	23
種類	合計							
Min	245.225(ms)	245.382	245.225	252.679	459.320	461.104	251.444	248.328
Max	1053.029(ms)	442.454	497.167	433.347	882.500	1053.029	957.153	935.343
Total	1514(回)	63	63	63	62	63	63	63
平均	310.685(ms)	295.191	292.323	290.763	594.254	618.365	458.965	303.542
普通	1056(69.75%)	44	50	42	0	0	24	46
少し遅い	252(16.64%)	15	11	6	0	0	5	15
遅い	122(8.06%)	3	2	1	20	45	25	2
timeout	84(5.55%)	1	0	14	42	18	9	0





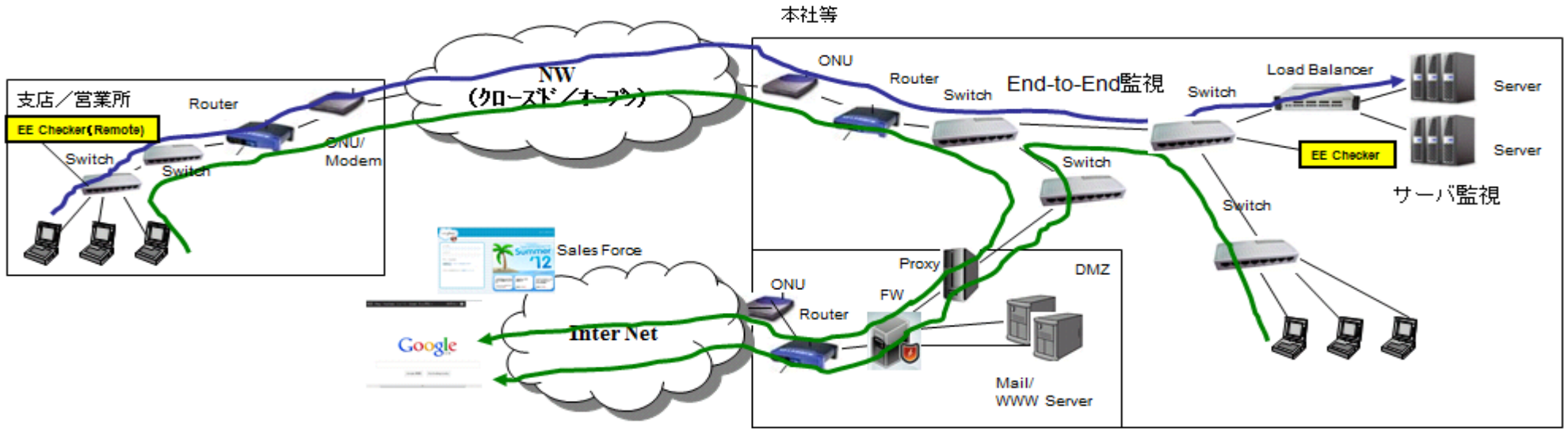
凡例　青色：普通　緑：少し遅い　紫：遅い　赤：timeout

参考2. 保守・運用サービスに必要なポイント（ポイント2）

クライアントからサーバまでの通し試験

ITインフラは、色々な機器、NWを利用しておりますので、単体の試験が良好でも、クアイアント（端末）～サーバ（クラウド等含み）の通しの試験が良好かどうか分かりません。

FWを超えた試験を含む、横方向の End to End試験 が必要

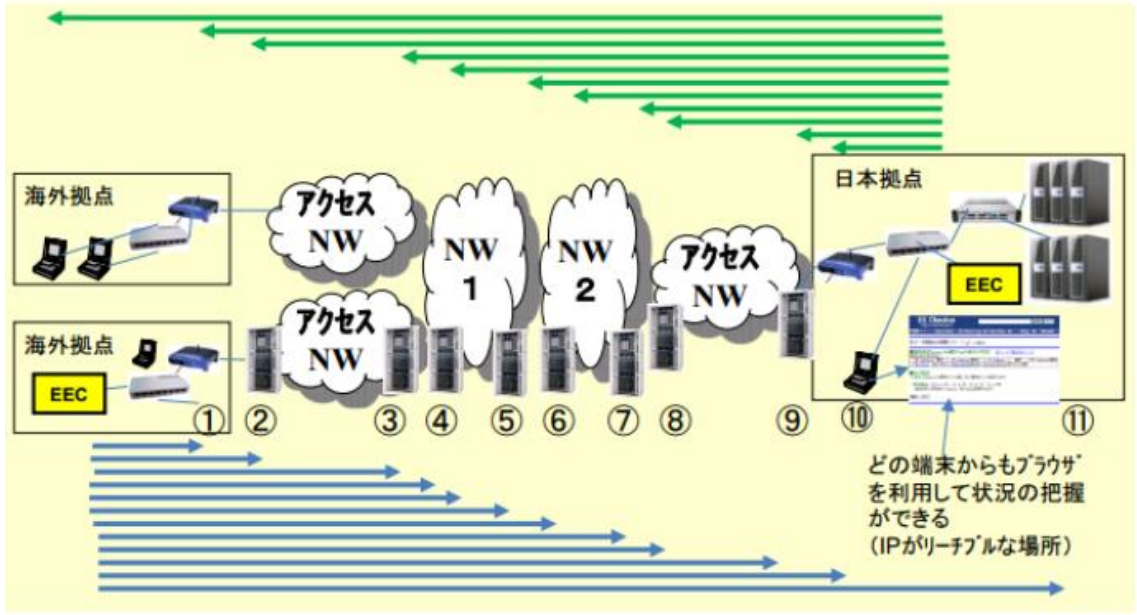


①各種機器を通ることにより、自ら故障情報を出せないメディアコンバータ、ケーブルのトラブルも発見できます。

②経由する機器が冗長構成になっている場合の故障も、常時監視することにより、不具合を発見できます。
特に発見しにくい故障は、冗長機器の１つが時々故障になるといったイレギュラーな場合で、**常時監視により、過去のデータのログを比較することによりトラブルを発見することが出来ます。**

参考2.1 クライアントからサーバまでの通し試験

お客さまが利用されているネットワークインフラは、いくつもの機器、ネットワークキャリアを経由するため、どの部分で故障かどうかの切り分けが課題となっていますが、End to End試験で異常部分の特定化ができます。

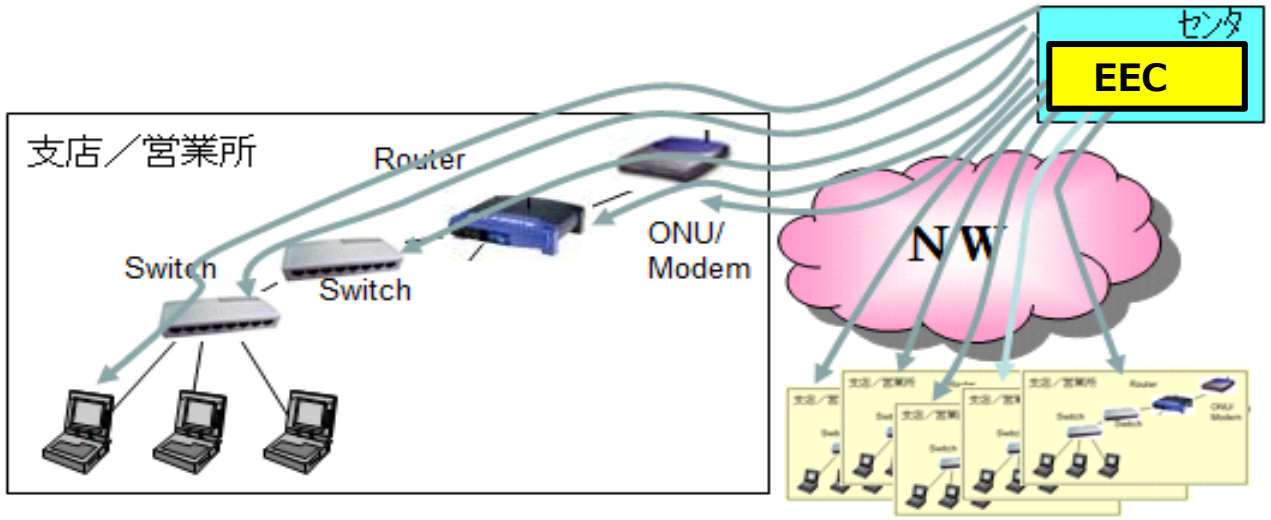


海外拠点のEECから日本拠点にping監視を行い異常部分の特定化を実施

参考3. 保守・運用サービスに必要なポイント（ポイント3）

全機器の監視

いつ、機器、NWにトラブルがあるか分からないので
できるだけ多くの機器の常時監視を行うことが有効



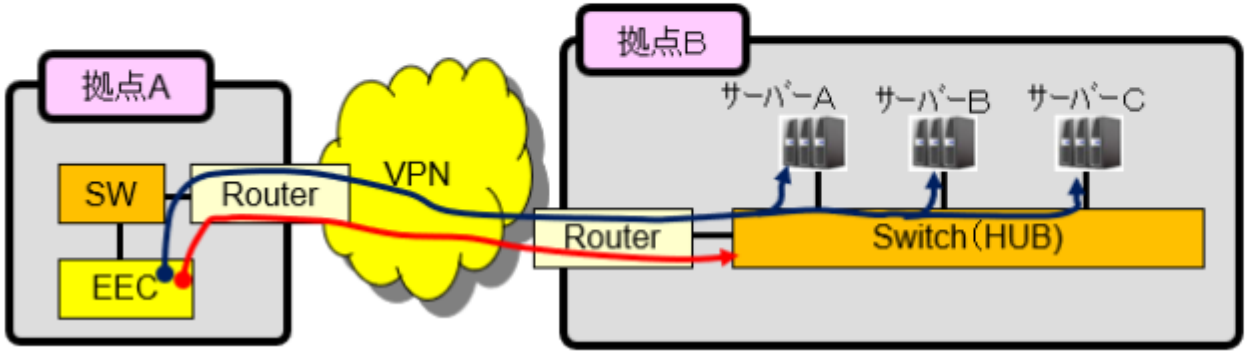
- **ITインフラ可視化分析サービスでは、監視をしないで急なトラブルの対応を行うより、できるだけ沢山のノードを常時監視し、緊急な対応を減らすことにより保守価格をリーズナブルなものにしています。**

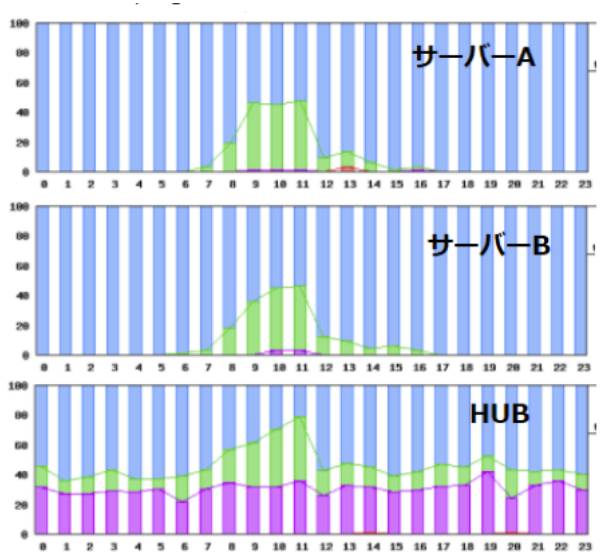
★全てのトラブルを、エンドユーザ様の申告前に発見できれば、対応を余裕を持って行うことができます。

★品質改善フローにより、トラブルになる前に対応することにより、保守価格を下げる努力をしております。

参考3.1 全機器の監視

Ping監視では、WAN越えのRouterへの試験が一般的ですが、Router配下の24時間連続運転の機器へのpingは、潜在故障発見に有効です。





サーバーA

時刻指定		00	01	02	03	04	05	06	07	08	09	10
種類	合計											
Min	6.319(ms)	6.327	6.466	6.618	6.319	6.493	6.595	6.436	6.820	6.472	7.119	6.991
Max	35.021(ms)	8.415	8.508	8.517	9.275	8.923	8.871	8.336	18.690	25.152	35.021	28.114
Total	1627(回)	70	70	70	69	70	70	70	68	67	67	67
平均	8.546(ms)	7.165	7.166	7.358	7.539	7.413	7.434	7.459	7.863	10.150	12.846	12.795
普通	1497(92.01%)	70	70	70	69	70	70	70	66	54	36	37
少し遅い	124(7.62%)	0	0	0	0	0	0	0	2	13	30	29
遅い	4(0.25%)	0	0	0	0	0	0	0	0	0	1	1
timeout	2(0.12%)	0	0	0	0	0	0	0	0	0	0	0

Switch（HUB）

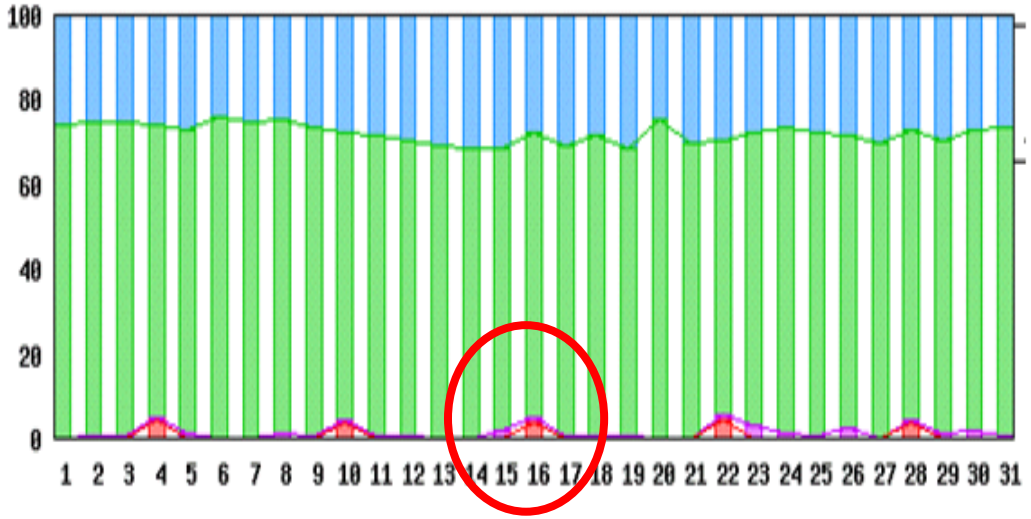
時刻指定		00	01	02	03	04	05	06	07	08
種類	合計									
Min	19.571(ms)	19.682	19.923	19.823	20.165	19.995	19.571	19.623	19.969	19.762
Max	320.930(ms)	186.081	151.330	188.998	132.335	130.172	139.472	125.155	128.956	106.986
Total	1627(回)	70	70	70	69	70	70	69	69	67
平均	37.433(ms)	39.651	36.684	34.486	37.548	33.090	34.821	32.124	36.633	38.796
普通	872(53.60%)	38	45	43	39	44	44	42	39	29
少し遅い	257(15.80%)	10	6	8	10	6	5	12	9	15
遅い	496(30.49%)	22	19	19	20	20	21	15	21	23
timeout	2(0.12%)	0	0	0	0	0	0	0	0	0

参考4. 保守・運用サービスに必要なポイント（ポイント4）

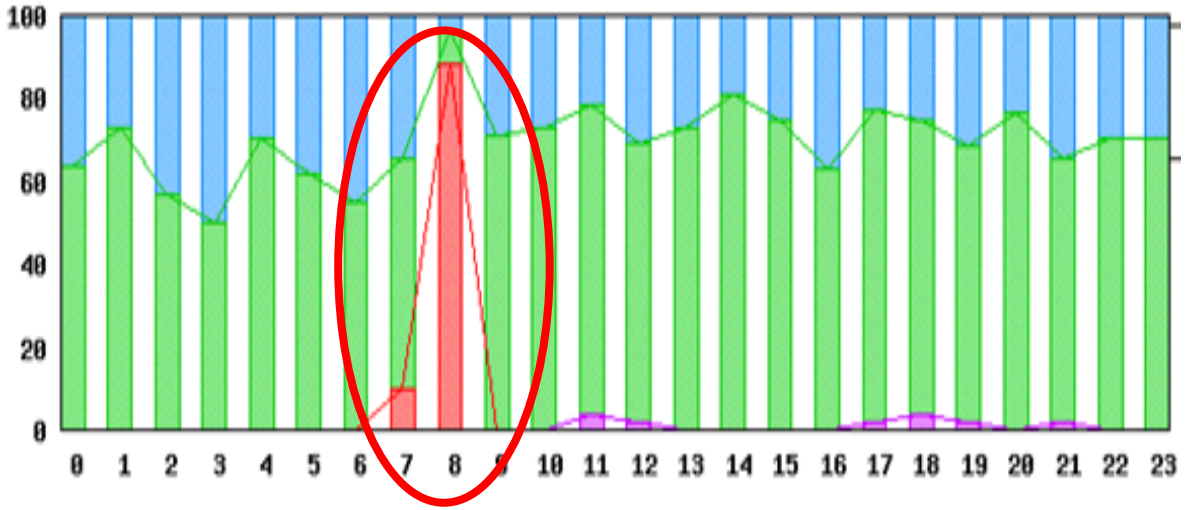
常時監視

常時監視したログ情報を見ることにより、見過ごされていたトラブルの発見に繋げることが可能

月データ　４日、１０日、１６日と定期的に故障



日データ　　７、８時台にtimeoutが発生



故障をしていない時にどんなに検証試験（ネットワークや、被疑機器の借用をしての確認試験）を行っても発見できませんが、
常時監視したログ情報を見ることにより、トラブルの発見に繋げることが可能です。

常時、且つなるべく多くの機器を監視しておくことが、見過ごされていたトラブルの発見に繋がる