

ネットワークエビデンスサービスについて

2025年

ITSコンサルティング株式会社

1. 会社概要
2. サービス概要
3. Web会議分析例
4. InterNet接続が遅い分析例
5. お客様が遅延と感じる原因の発見例
6. 最後に

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

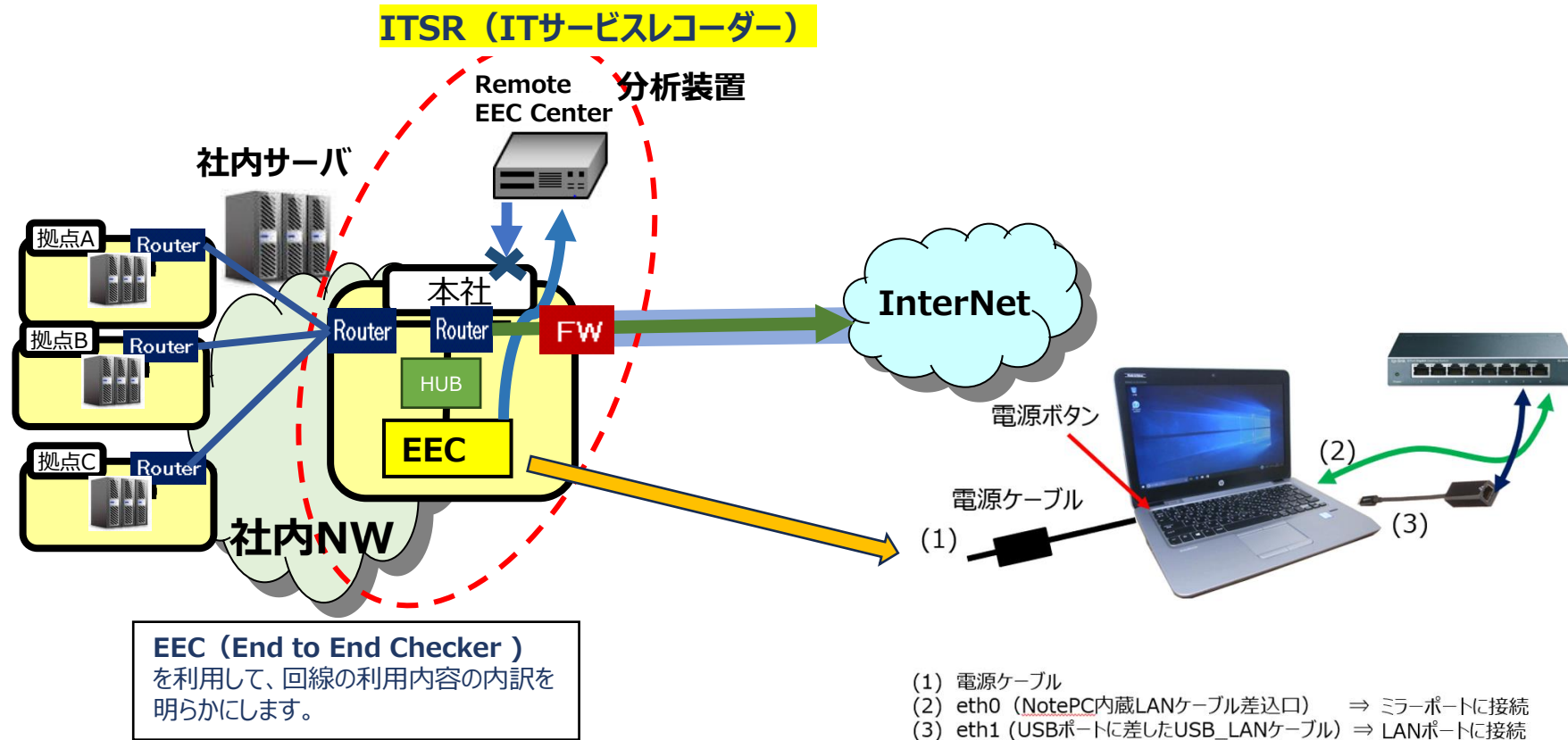
会社情報

[■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 ネットワークエビデンスサービスとは

ネットワークエビデンスサービスとは、
「ネットワークが混みだしているが、何に使っているかが判らないので、
増速するかどうかの判断が付かない」と云うお客様のお悩みを解決するサービスです

お客様の拠点にEECを設置させて頂き、パケットキャプチャーによる通信内容の分析、
及びsnmp情報によるトラフィック情報の可視化を行い、ネットワーク利用内容を明らかにし、
ネットワーク帯域が妥当かの証拠（エビデンス）を作成します。



ネットワークエビデンスサービスには、パケットキャプチャーと併せてエビデンスを取るための幾つかの機能が有りますので、お客様の状況に合わせて組み合わせて使用します。

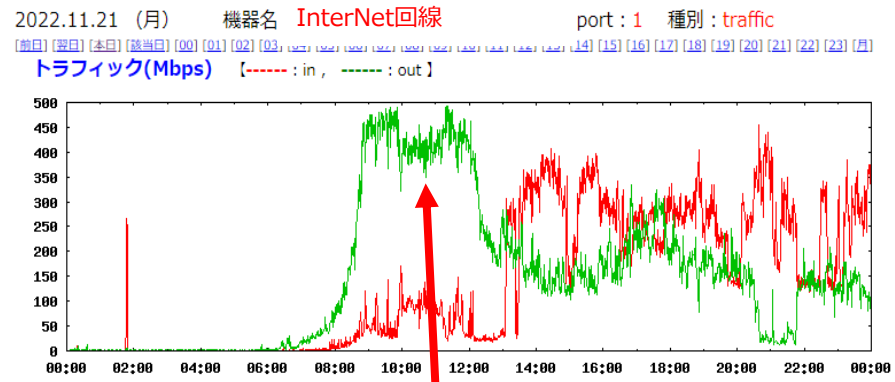
サービス内容
① EECを使用したネットワークエビデンスサービス
・パケットキャプチャー
・snmp情報によるトラヒック情報の可視化
・Ping監視
・ポート試験
・http,https試験
・4 WEB試験
② 取得したデータの分析レポートサービス
・分析レポート作成
・オンラインによる分析レポートの説明

***Ping監視、http、https試験等には監視ポイントの制限はありません。**

SNMP（トラフィック情報） + Ping監視により ネットワーク状況が判明

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

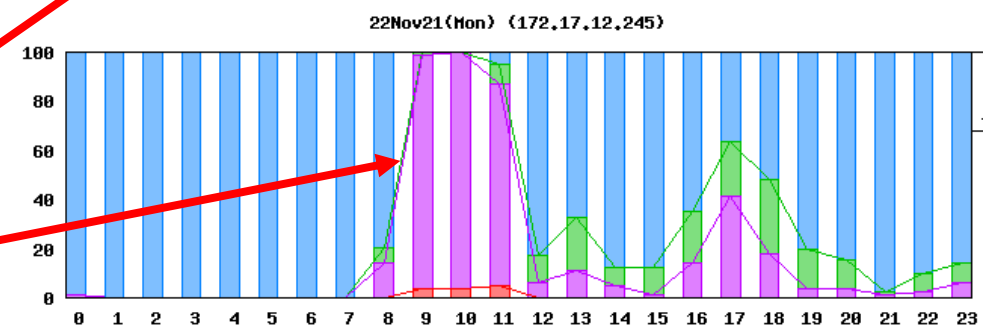
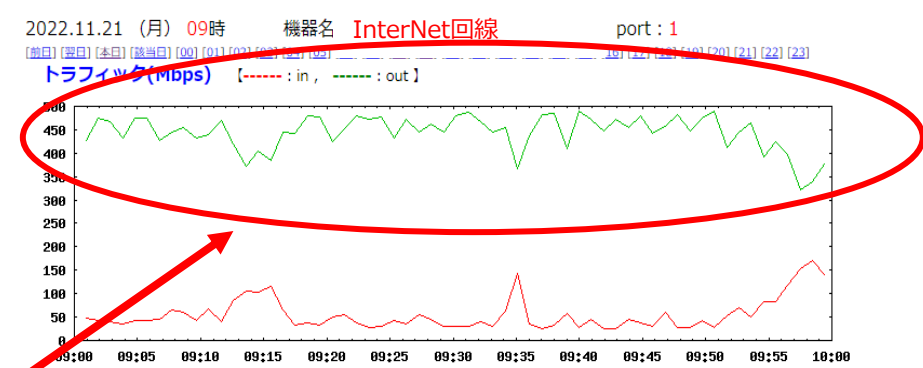
11月21日のトラフィック状況（1分平均）



時刻指定		07	08	09	10	11	12
種類	合計						
Min	3.762(ms)	3.920	3.838	17.516	30.450	3.928	3.793
Max	207.098(ms)	4.297	53.068	65.336	90.389	69.027	66.273
Total	1907(回)	80	79	80	79	79	80
平均	12.572(ms)	4.080	10.642	48.398	55.028	42.752	38.277
普通	1430(74.99%)	80	63	0	0	0	66
少し遅い	147(7.71%)	0	0	1	0	6	9
遅い	320(16.78%)	0	1	76	76	65	5
timeout	10(0.52%)	0	0	3	3	4	0

timeoutが発生

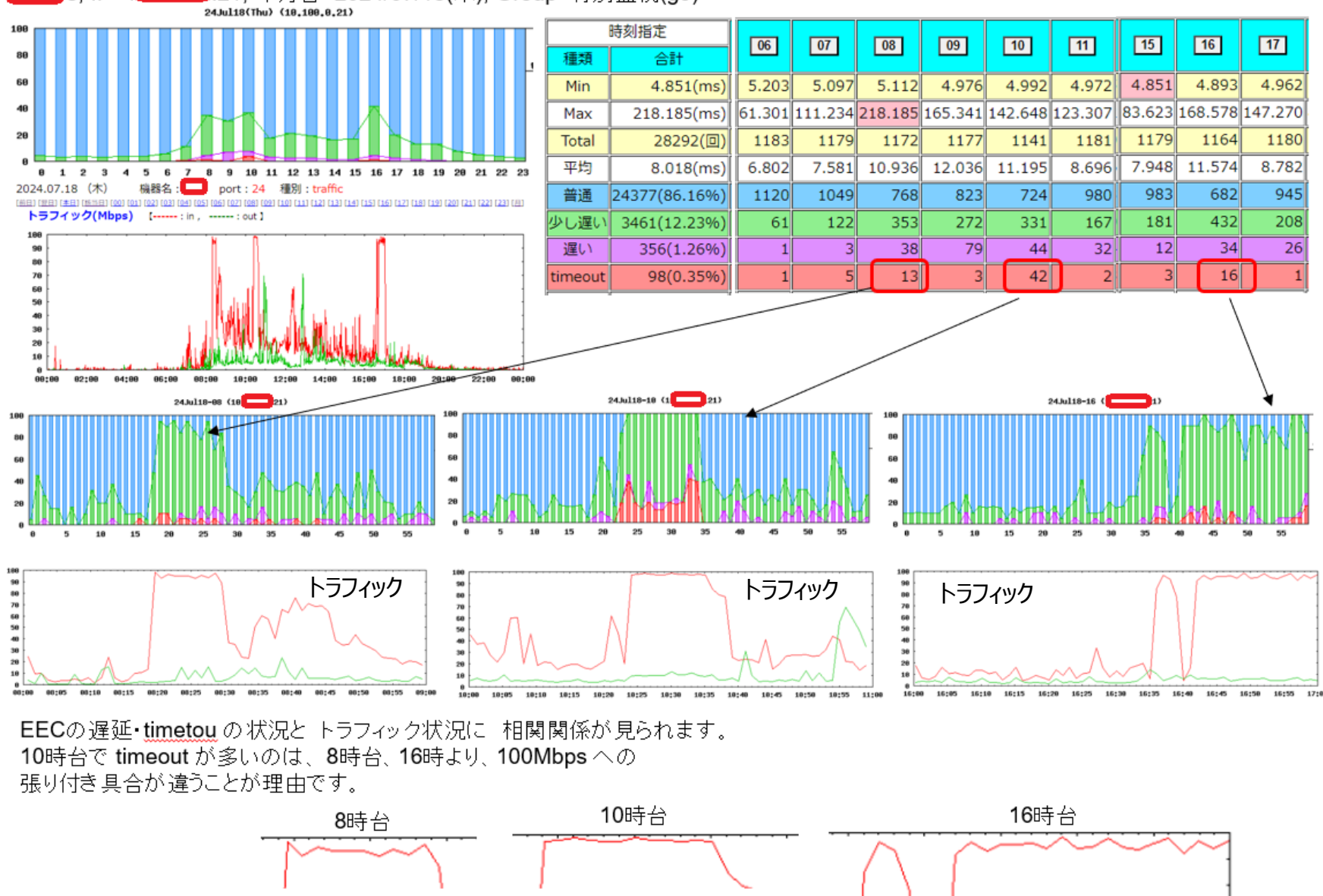
9時台のトラフィック状況



2.4 トラフィック情報とPing監視状況の相関性について

他のお客様の例 EECの試験結果で遅延・timeout があると、回線ひっ迫の可能性あります。

e, IP=1.21, 年月日=2024/07/18(木), Group=特別監視(g5)



2.5 ネットワーク利用内容の分析の容易化

1000万パケット5世代分のデータを保管し
その中のデータをお客様自身でも容易に分析可能
(誰が何処へ接続して、何の通信を行っていたかが判ります)

パケットキャプチャーの
データをEECで分析

パケットキャプチャーで
収集したデータ



No	発IP	packet数	%
1	225.110.10	732944	38.5
2	12.179.236	163750	8.6
3	122.42.48	131906	6.9
4	11.225.241	103639	5.4
5	211.176.9	49380	2.6
6	11.176.140	47567	2.5
7	211.176.45	37197	2.0
8	211.176.31	35967	1.9
9	211.176.36	35952	1.9
10	211.176.33	34079	1.8
11	211.176.71	27807	1.5
12	211.176.97	27697	1.5
13	211.176.85	26764	1.4
14	11.176.128	25323	1.3
15	11.176.149	25265	1.3
16	211.23.241	25016	1.3
17	11.176.240	21175	1.1
18	11.176.109	17802	0.9

No	着IP	packet数	%
1	225.110.10	681695	36.5
2	11.225.241	69709	3.7
3	11.176.233	42078	2.3
4	11.176.110	42067	2.3
5	211.176.4	41379	2.2
6	11.176.162	41291	2.2
7	211.176.8	39948	2.1
8	11.176.140	38711	2.1
9	211.176.9	37988	2.0
10	11.176.128	34575	1.9
11	11.176.107	34361	1.8
12	211.176.45	29834	1.6
13	211.176.31	29237	1.6
14	211.176.33	27231	1.5
15	211.176.97	26952	1.4
16	211.176.36	26277	1.4
17	211.93.50	24650	1.3
18	11.176.148	23129	1.2

No	発プロトコル	packet数	%
1	http	764045	41.4
2	cleanerliverc	158607	8.6
3	twrpc	133361	7.2
4	microsoft-ds	117529	6.4
5	49688	17361	0.9
6	https	15500	0.8
7	49701	9982	0.5



No	着プロトコル	packet数	%
1	http	693651	40.4
2	microsoft-ds	83669	4.9
3	50055	44441	2.6
4	50045	28661	1.7
5	50007	26457	1.5
6	49701	24265	1.4
7	50056	20765	1.2

No.	Time	Source	Destination	Protocol	Length	Info
220371	15:23:51.171046	192.168.200.11	192.168.50.101	KRBS	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 capture]
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	KRBS	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	KRBS	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	492	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

Packet数の多いipアドレス（TOP10）の利用状況を、混雑日（例.毎週月曜日）の指定時間帯（例.8時～10時台）での推移を表示します。

週明けの月曜（or火曜：月曜が祝日の場合）の 11:00（現時点）に パケットキャプチャーデータを保存し、約 6,000万パケット弱のデータを分析し、TOP発、着IPについて、パケットの推移を表示します。

例は、6/3（月）の検索結果です。

データの取得日（過去2カ月）

該当日：2024 年 06 月 03 日 (月)

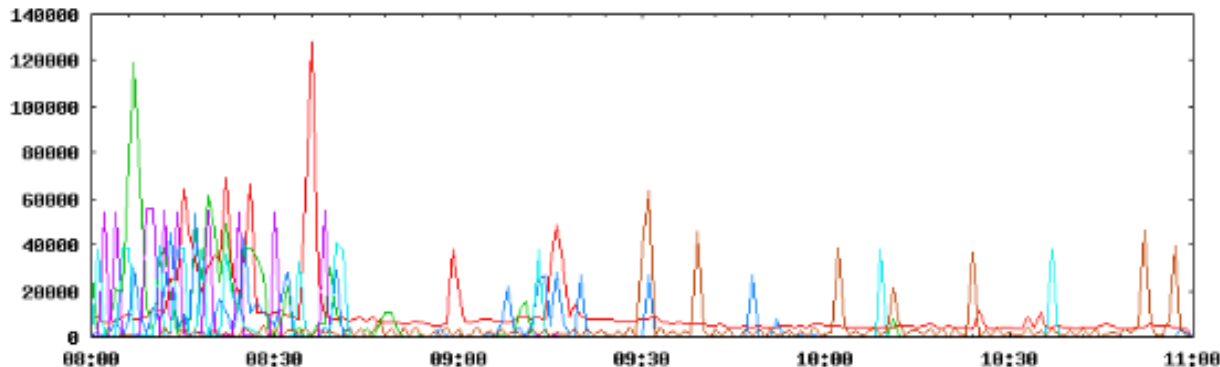
発IP TOP 10 【Defaultを表示】 【Packet Data 時間帯：07:53～11:00】

☒ [1] A_Server ☒ [2] ☒ [3] ☒ [4] ☒ [5] ☒ [6] B_Server
☐ [7] ☐ [8] ☐ [9] C_Server ☐ [10] ☐ [11] その他 ☐ [12] 合計

時刻の表示 【Defaultの表示】

☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☒ 8 ☒ 9 ☒ 10 ☒ 11
☒ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23

↑を選択して 再表示 をクリックすると 選択された項目が表示されます



<<データの時間帯>>

5世代+0世代（今取得中の世代）
の全データの時間帯です。

このお客様は、1世代、1,000万パケット
ですので、5,000～6,000万パケットが、
約3時間のパケット量になります。

2.7 Packet推移のグラフによる絞込

該当日：2024年06月03日(月)

発IP TOP 10 【選択した項目を表示】 【Packet Data 時間帯：07:53～11:00】

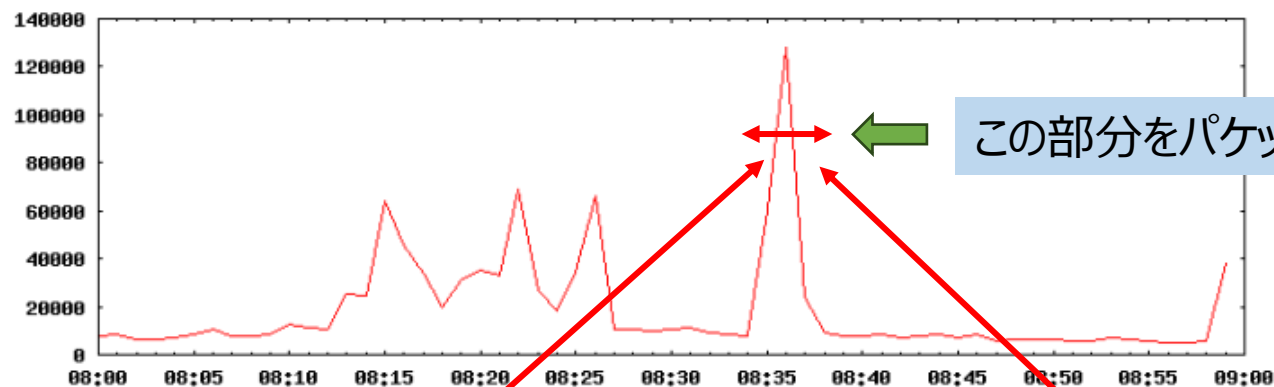
☒ [1] A_Server ☐ [2] 232.240 ☐ [3] 110.172 ☐ [4] 117.85 ☐ [5] 117.217 ☐ [6] B_Server
☐ [7] 80.100 ☐ [8] 114.172 ☐ [9] C_Server ☐ [10] 27.128 ☐ [11] その他 ☐ [12] 合計

時刻の表示 【選択した項目を表示】

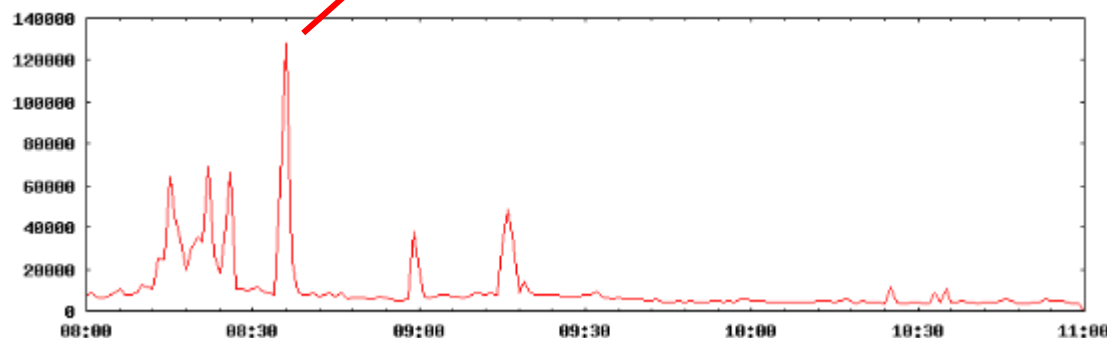
☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☒ 8 ☐ 9 ☐ 10 ☐ 11
☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ 21 ☐ 22 ☐ 23

再表示

↑を選択して 再表示 をクリックすると 選択された項目が表示されます



赤枠の部分のみ選択して、再表示をした結果です。



一番パケット数の多いipアドレスのみを指定し、再表示し、更にパケット数が多い8時台を表示

2.8 Packet推移のグラフからのipアドレスの絞込

絞込 : A_Serverのipアドレス

パケット時間帯 : 2024-06-03 08:34:38 ~ 08:36:37【 1 分 59 秒 】



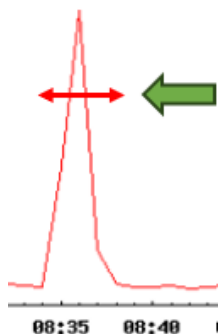
No	発IP	packet数	%
1	A_Server	176083	75.0
2	X_パソコン	40710	17.3
3	10.13	1555	0.7
4	10.13	1311	0.6
5	10.13	1021	0.4
6	10.13	952	0.4
7	10.13	877	0.4
8	10.13	857	0.4
9	10.13	751	0.3
10	10.13	680	0.3

No	着IP	packet数	%
1	X_パソコン	147118	63.1
2	A_Server	70868	30.4
3	10.13	1589	0.7
4	10.13	996	0.4
5	10.13	778	0.3
6	10.13	732	0.3
7	10.13	566	0.2
8	10.13	516	0.2
9	10.13	511	0.2
10	10.13	419	0.2

No	発プロトコル	packet数	%
1	52300	164232	70.3
2	59385	39296	16.8
3	52304	11356	4.9
4	59175	1357	0.6
5	53008	1283	0.5

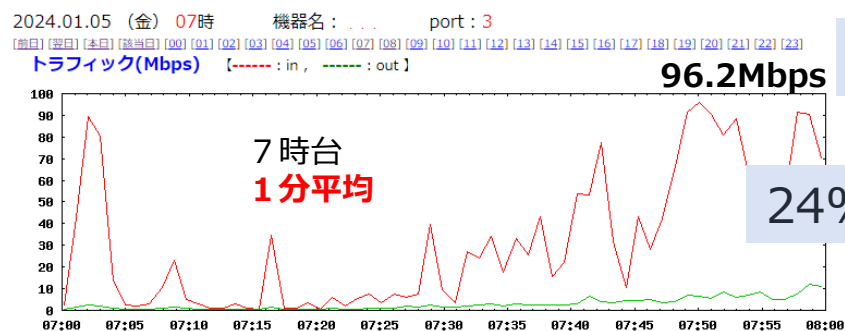
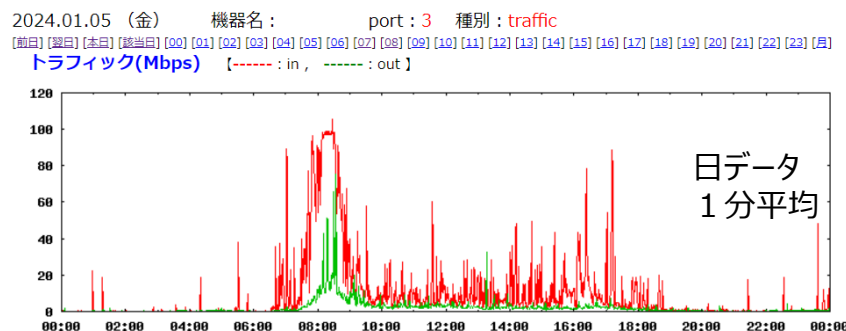


No	着プロトコル	packet数	%
1	59385	145955	62.9
2	52300	61028	26.3
3	52304	9832	4.2
4	59175	1095	0.5
5	55241	878	0.4
6	53008	745	0.3



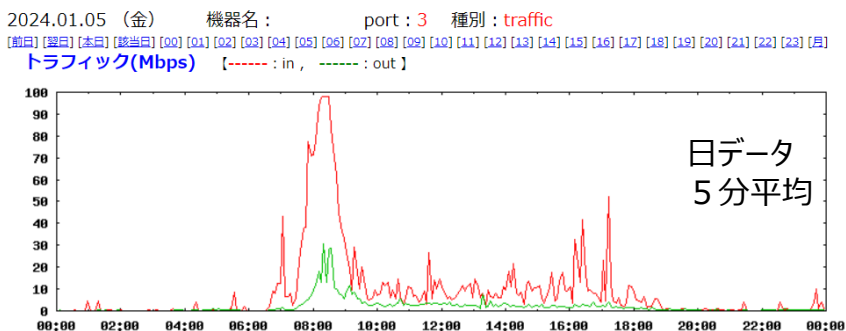
8:35ごろ、
A_Server は、X_パソコンと
かなりの通信を行っていることが分かります。

1分平均のトラフィック情報（SNMP情報）により お客様のネットワーク体感速度に近い帯域の測定を実現

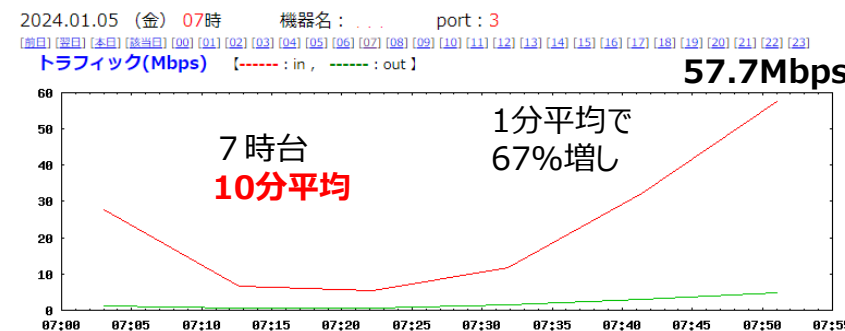
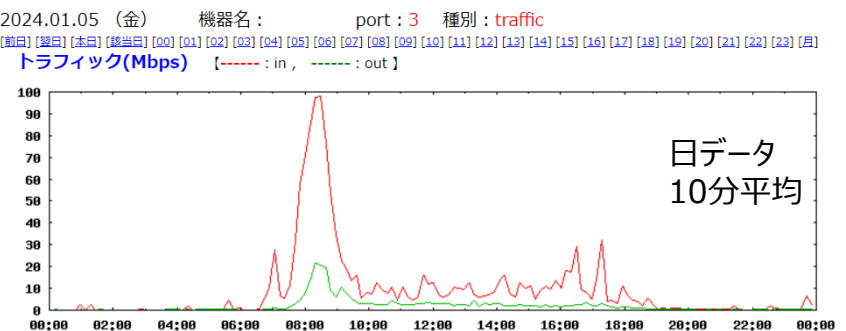


67%増

24%増



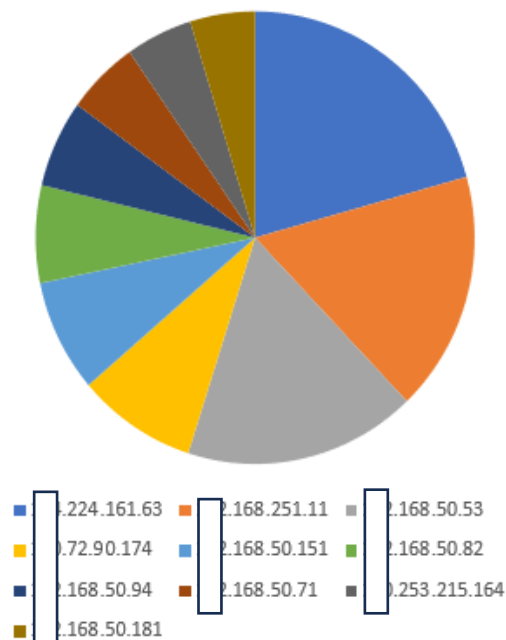
34%増



Web会議中の音声が届かないとの事で、調査を実施

13:57:46 ～ 14:55:52の全時間帯において
使用中のIPをPacket数順に分析

No	IP	packet数	メモ	%	相手先を含めた%
1	224.161.63	2,879,697	Zoom	16.1	32.3
2	168.251.11	2,394,273		13.4	
3	168.50.53	2,380,160		13.3	
4	72.90.174	1,222,406	Webex	6.8	
5	168.50.151	1,123,986		6.3	
6	168.50.82	969,927		5.4	
7	168.50.94	869,552		4.9	
8	168.50.71	741,897		4.2	
9	253.215.164	684,631	Webex	3.8	
10	168.50.181	666,267		3.7	
11	168.50.130	488,092		2.7	
12	168.50.52	467,433		2.6	
13	168.50.76	359,907		2.0	
14	63.35.157	357,486	USEN	2.0	
15	168.100.206	303,672		1.7	
16	168.50.57	244,659		1.4	
17	168.50.128	238,830		1.3	
18	72.56.181	219,794	Webex	1.2	
19	168.50.157	199,211		1.1	



WebEXを利用している方も存在します。

WebEXとZoomパケット量と通信量の比較分析

No	新ファイル名	試験時間 開始 ~ 終了			時刻差	WebEX			Zoom		
						パケット数	length (byte)	length累計 (byte)	パケット数	length (byte)	length累計 (byte)
1	B_P_211104.cap	13:57:46	~	13:58:26	0:00:40	2,525	2,161,649	2,161,649	35,163	19,061,991	19,061,991
2	B_P_211104.cap1	13:58:26	~	13:58:43	0:00:17	0	0	2,161,649	15,118	7,980,452	27,042,443
3	B_P_211104.cap2	13:58:43	~	13:59:16	0:00:33	11	6,293	2,167,942	32,219	17,564,463	44,606,906
4	B_P_211104.cap3	13:59:16	~	13:59:42	0:00:26	35	0	2,167,942	41,333	21,320,873	65,927,779
5	B_P_211104.cap4	13:59:42	~	14:00:17	0:00:35	55	16,460	2,184,402	45,423	20,901,987	86,829,766
6	B_P_211104.cap5	14:00:17	~	14:00:50	0:00:33	0	0	2,184,402	36,258	22,304,385	109,134,151
7	B_P_211104.cap6	14:00:50	~	14:01:29	0:00:40	8	6,118	2,190,520	38,630	25,788,112	134,922,263
8	B_P_211104.cap7	14:01:29	~	14:02:12	0:00:42	11	5,966	2,196,486	43,208	29,797,948	164,720,211
100	B_P_211104.cap99	14:52:43	~	14:53:29	0:00:46	44,891	21,459,969	475,454,031	8,150	5,725,526	1,561,771,180
101	B_P_211104.cap100	14:53:29	~	14:54:12	0:00:43	40,958	19,765,018	495,219,049	21,994	17,927,189	1,579,698,369
102	B_P_211104.cap101	14:54:12	~	14:54:46	0:00:35	32,333	15,881,683	511,100,732	26,987	21,277,805	1,600,976,174
103	B_P_211104.cap102	14:54:46	~	14:55:18	0:00:31	29,507	14,622,274	525,723,006	30,936	23,098,738	1,624,074,912
104	B_P_211104.cap103	14:55:18	~	14:55:52	0:00:34	32,088	15,497,235	541,220,241	29,823	19,042,791	1,643,117,703

累計通信量byte→ 541,220,241

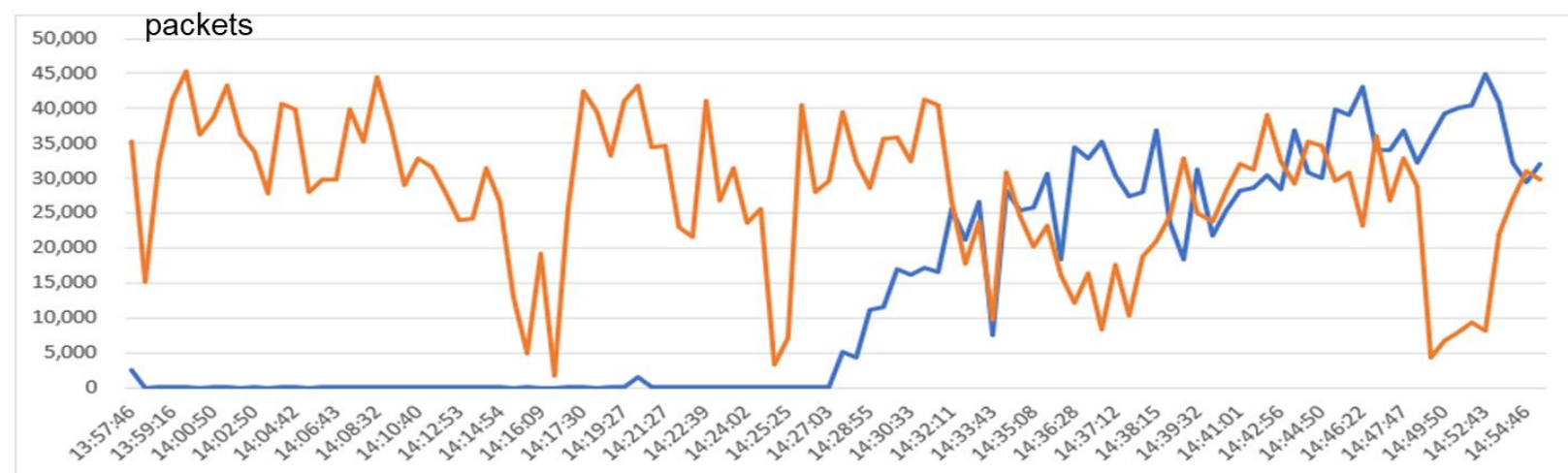
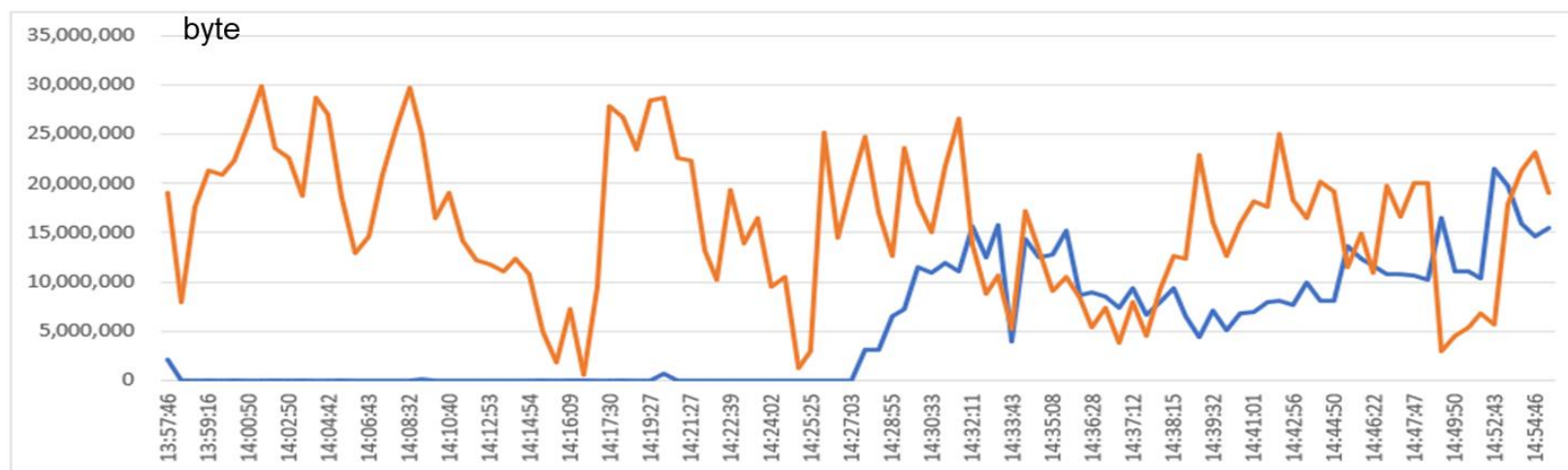
累計通信量byte→ 1,643,117,703

3.3 WebexとZoomのWeb会議利用時の比較_2

WebEXとZoomのパケット量と通信量をグラフ化しましたが、パケット量の差はあまり無いが、WebEXの方が通信量が少ない。

13:57:46 ~ 14:55:52の全時間帯における
WebEXとZoomのパケット量、及び通信量 (byte) の分析グラフ

— WebEX — Zoom



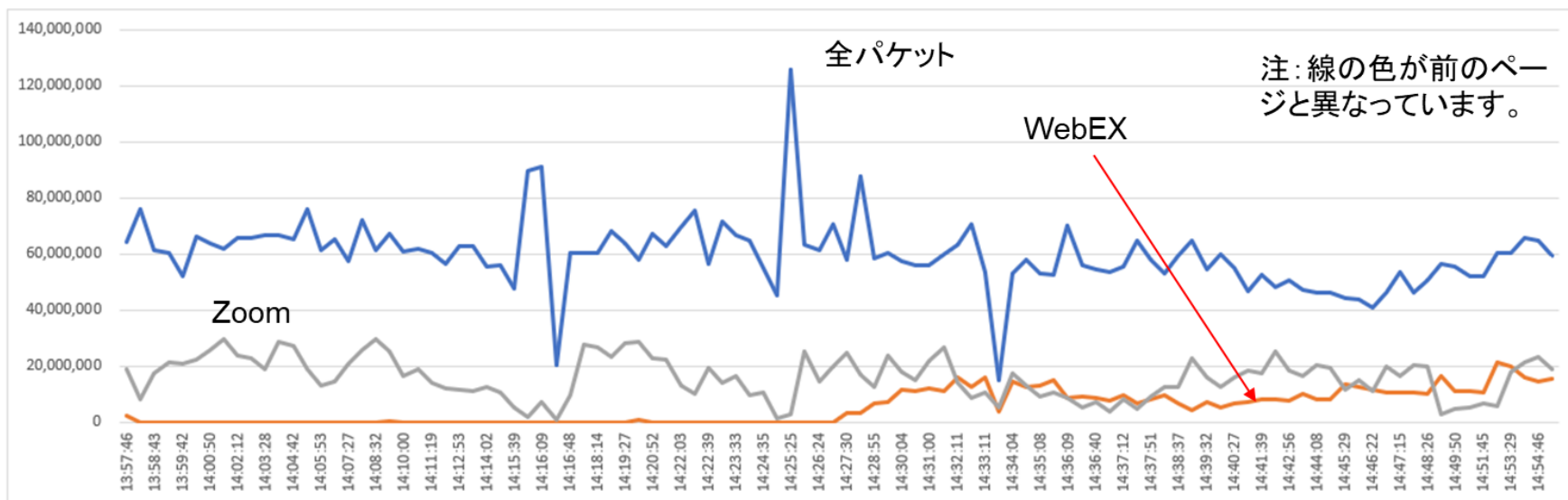
3.4 Web会議を行うための回線帯域の調査

お客様は、フレッツ回線（IPoE）を使用しているのですが、回線帯域が不足して音声途切れるのではと心配していたので、全体通信量に占めるWeb会議の通信量を出したが、Web会議は30%程度の利用なので、問題無い事を説明。

13:57:46 ~ 14:55:52の全時間帯における
全パケットに占めるWebEXとZoomのパケット量の分析

No	新ファイル名	試験時間			時刻差	全パケット	WebEX	Zoom
		開始	～	終了		length (byte)	length (byte)	length (byte)
1	B_P_211104.cap	13:57:46	～	13:58:26	0:00:40	64,165,395	2,161,649	19,061,991
2	B_P_211104.cap1	13:58:26	～	13:58:43	0:00:17	75,884,657	0	7,980,452
3	B_P_211104.cap2	13:58:43	～	13:59:16	0:00:33	61,308,696	6,293	17,564,463
4	B_P_211104.cap3	13:59:16	～	13:59:42	0:00:26	60,141,126	0	21,320,873
103	B_P_211104.cap102	14:54:46	～	14:55:18	0:00:31	64,796,105	14,622,274	23,098,738
104	B_P_211104.cap103	14:55:18	～	14:55:52	0:00:34	59,086,822	15,497,235	19,042,791
						6,204,302,769	541,220,241	1,643,117,703

bytes



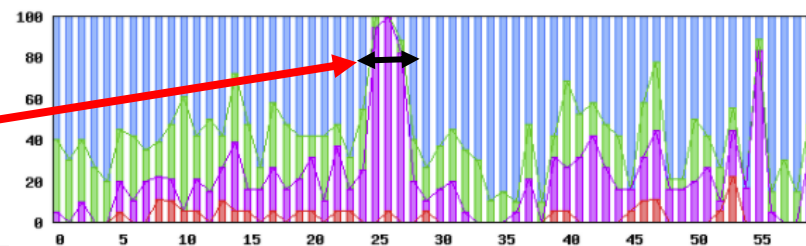
3.5 Web会議中に音声途切れる原因

Web会議中、帯域を多く使用するファイル転送を行っていることから、Web会議用の帯域が狭まり、音声の送受信帯域がごく僅かになった時、音声途切れました。

192.168.50.101 の通信について

No	新ファイル名	試験時間			時刻差	全パケット			192.168.50.101		
		開始	～	終了		パケット数	length (byte)	length累計 (byte)	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

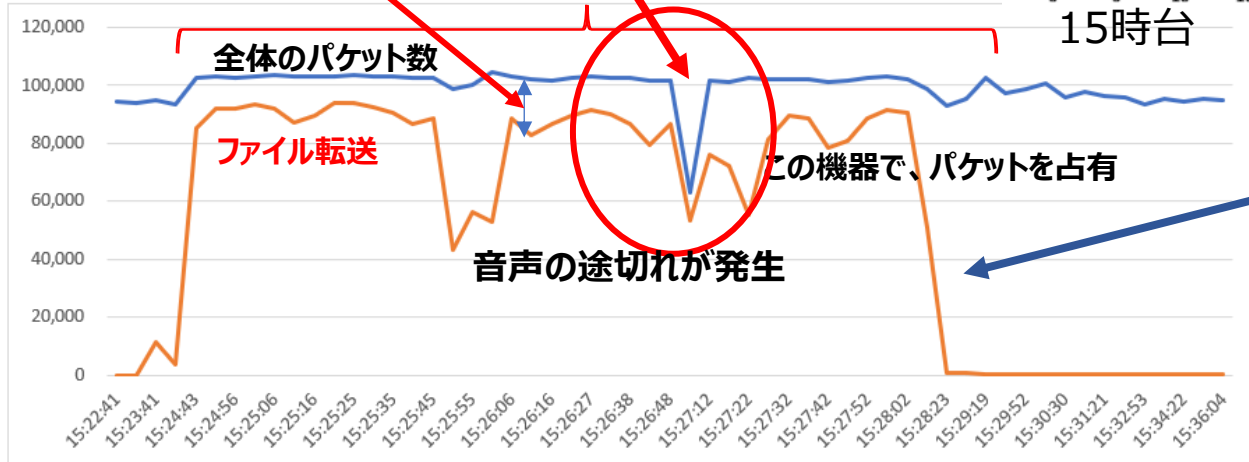
21Nov04-15 (202,239,113,19)



15時台

Web会議は、この帯域で実施

遅延と対応

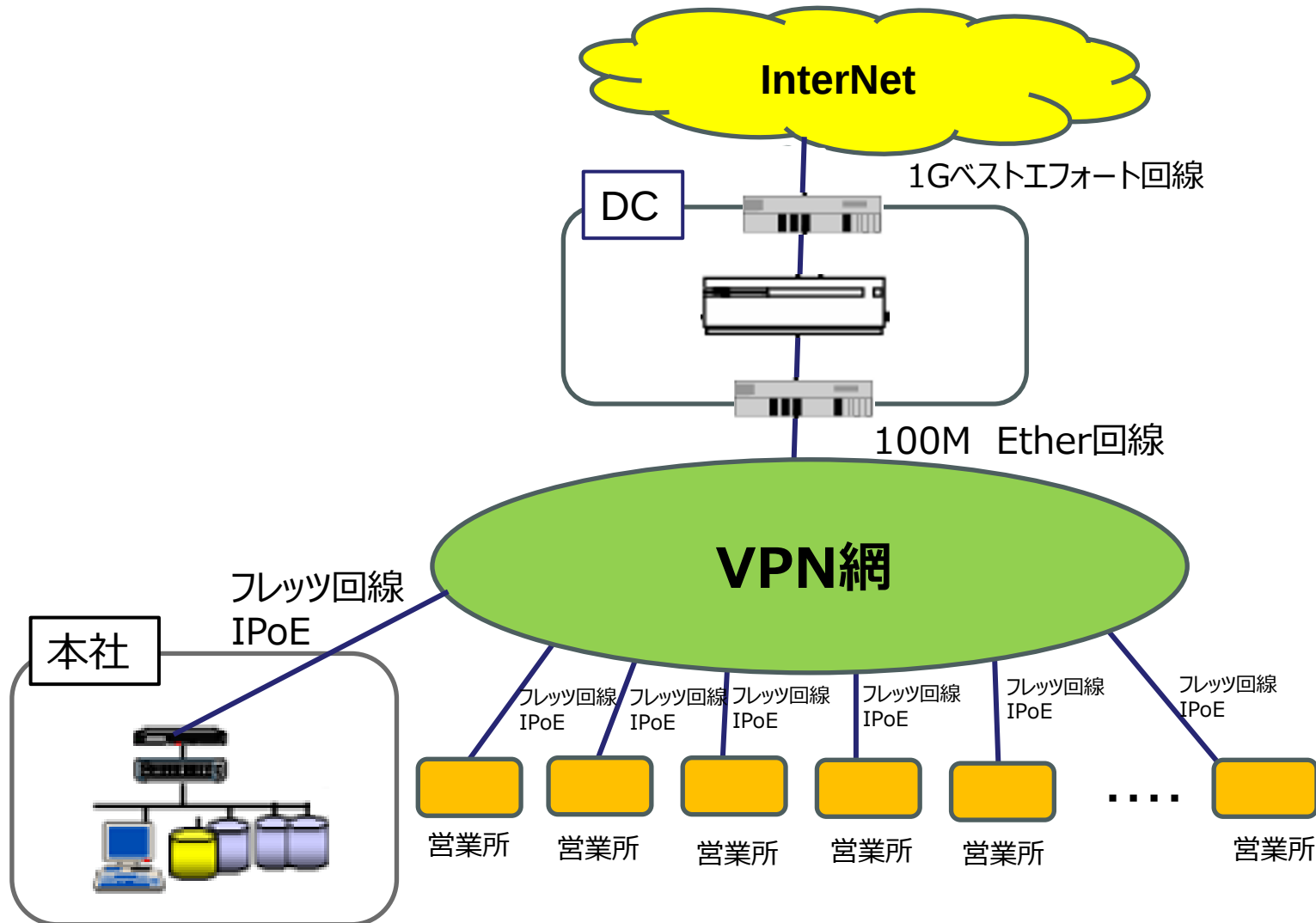


調査結果

Web会議中にファイル転送を行う方がいて、Web会議用の帯域が少なくなり、音声途切れた

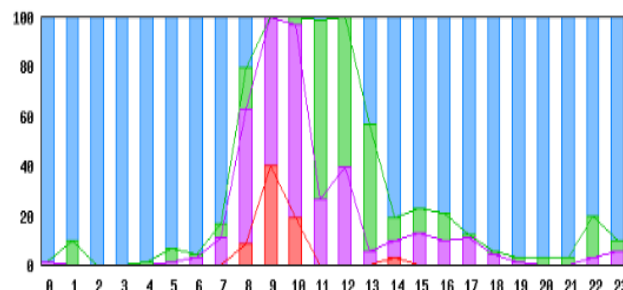
休み明けにInterNet接続を行うと遅いとの事で、調査を実施

お客様のシステム構成図

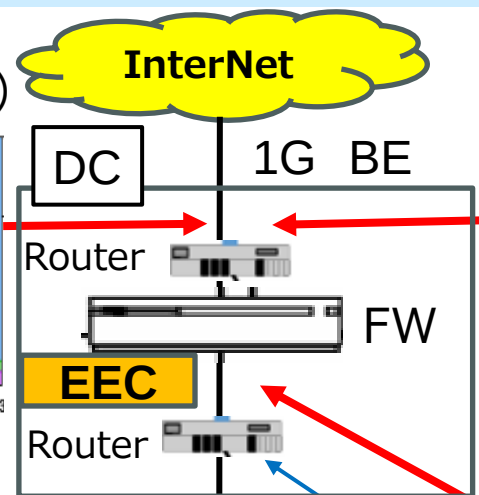
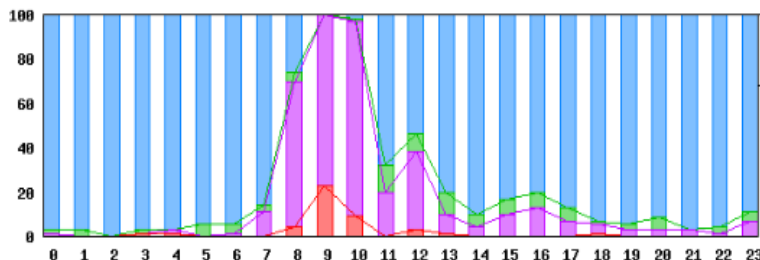


トラフィック情報とPing試験、Port試験結果を見ると、InterNet側からのトラフィックが100Mbpsを超えた時、Ping試験、Port試験でtimeoutが発生しました。LAN側Routerでパケットの破棄・遅延が発生したと思われます。

お客様のHPへのPort試験 (443)



本社 Ping試験



100M Ether回線

パケットの
破棄・遅延が発生

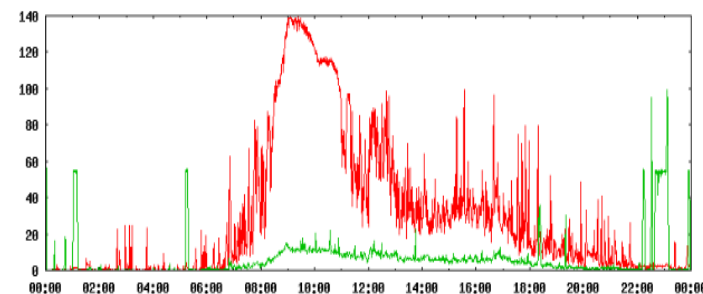
VPN網

フレッツ回線
IPoE

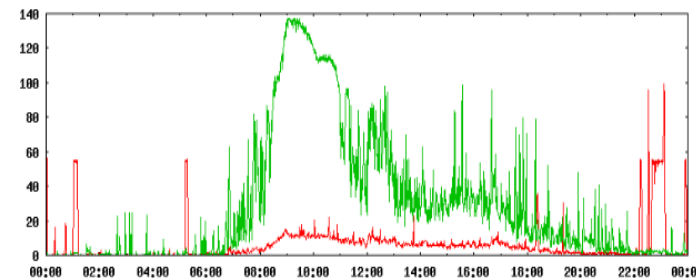
本社

InterNet回線のトラフィック

トラフィック(Mbps) [---: in, ---: out]



トラフィック(Mbps) [---: in, ---: out]



トラフィック増とtimeoutの相関関係が見られ、LAN側回線の帯域不足が判明。

4.3 Packet推移から通信内容の分析

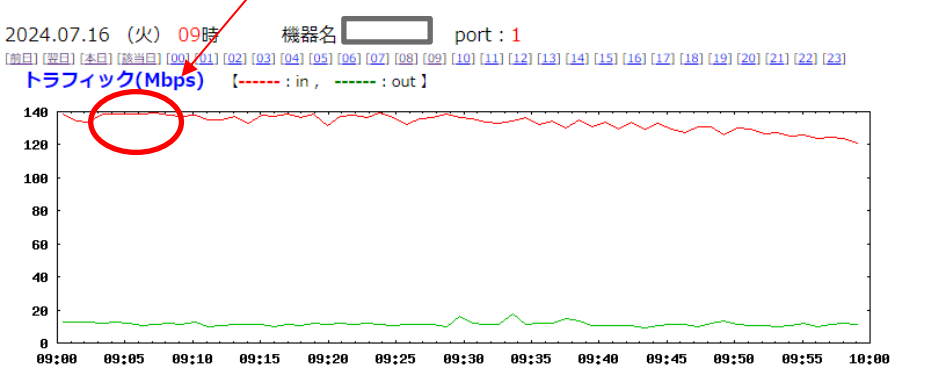
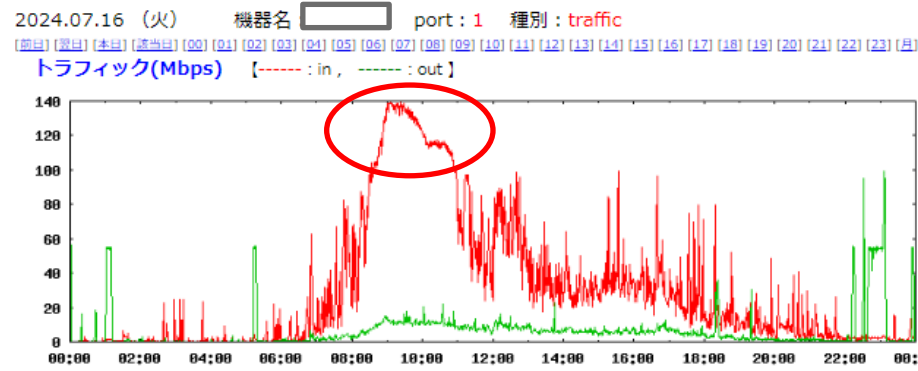
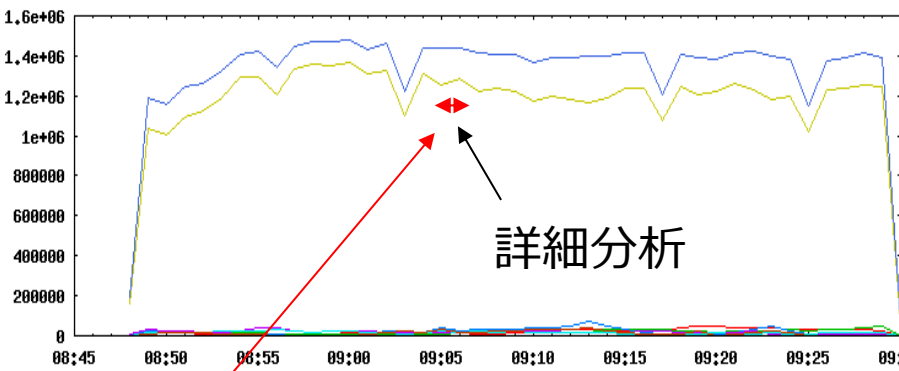
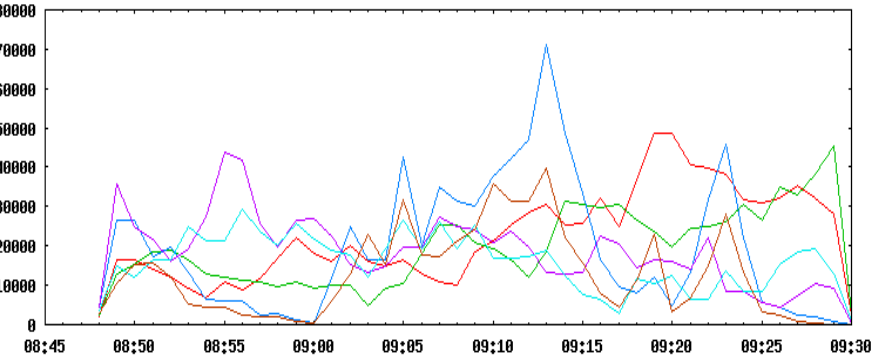
パケット推移を見るとInteNet回線からダウンロードは、140Mbps（FWでの収集なので100Mbps以上の数値）となっており、LAN側回線は100Mbpsに張り付いていました。
下りの回線帯域が100Mbps時の9時5分にどのような通信が行われていたかを分析し、通信内容により、回線増速の必要性を調査しました。

該当日：2024年07月16日(火)

発IP TOP 10 【選択した項目を表示】 【Packet Data 時間帯：08:48 ~ 09:30】

☒ [1] ☒ [2] ☒ [3] ☒ [4] ☒ [5] ☒ [6] ☒ [11] その他 ☒ [12] 合計

☐ [7] ☐ [8] ☐ [9] ☐ [10] ☐ [11] その他 ☐ [12] 合計



4.4 パケットキャプチャーで接続先確認

パケットキャプチャーデータをLAN側アドレスO.O.101.69で絞り込むと、Akamai, Microsoftとの通信と判明しました。Akamaiについても、Microsoft利用で使用していると思われます。

分析の結果、休み明けの9時台に使用しているアプリケーションを確認して頂き、増速することとなりました。

No	発IP	packet数	%
1	.101.69	8201	39.0
2	.70.156	2910	13.8
3	.185.90	2102	10.0
4	.185.91	1737	8.3
5	.185.92	1652	7.8
6	.185.81	1213	5.8
7	.252.135	1073	5.1
8	.185.82	727	3.5
9	.18.16	316	1.5
10	.90.34	206	1.0
11	.252.23	141	0.7
12	.70.162	117	0.6
13	.25.160	67	0.3
14	.7.201	58	0.3
15	.21.134	48	0.2
16	.12.159	46	0.2
17	.00.171	37	0.2
18	.58.89	29	0.1
19	.13.124	28	0.1
20	.70.146	28	0.1
21	.04.170	27	0.1
22	.3.7.79	22	0.1
23	.10.122	20	0.1

Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Akamai
Microsoft
Akamai
Akamai
Akamai
Microsoft

No	着IP	packet数	%
1	.101.69	12847	61.0
2	.70.156	1710	8.1
3	.185.90	1281	6.1
4	.185.91	1114	5.3
5	.185.92	1077	5.1
6	.185.81	766	3.6
7	.252.135	710	3.4
8	.185.82	453	2.2
9	.18.16	217	1.0
10	.90.34	152	0.7
11	.252.23	89	0.4
12	.70.162	80	0.4
13	.121.134	54	0.3
14	.7.201	48	0.2
15	.225.160	46	0.2
16	.100.171	30	0.1
17	.12.159	27	0.1
18	.13.124	23	0.1
19	.4.58.89	22	0.1
20	.63.7.79	22	0.1
21	.51.208	20	0.1
22	.10.122	20	0.1
23	.70.146	19	0.1

5. お客様が遅延とを感じる原因の発見例

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

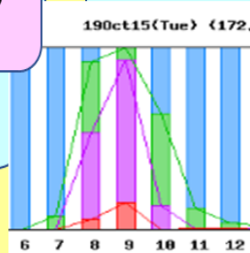
Routerにて、プッシュがある時間保持のため遅延が発生

他の機器に起因すること

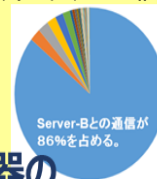
他機器の影響
WidowsUP関連

ベストエフォートで
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



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



帯域に関すること

お客様要望
「帯域不足は理解できたが、どのようなパケットで、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」

遠隔でパケットキャッチャーを実施し、分析。
お客様は納得して、増速に至る。

ギランティ回線 (UNO)しか
トラフィックレポートが出せない。
⇒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

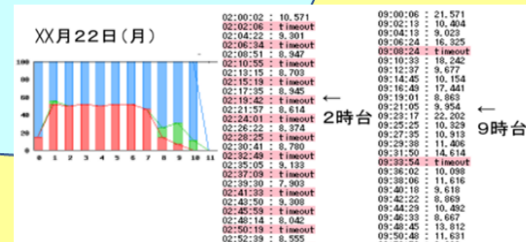
SalesForce
の遅延例

Office365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



**ネットワークエビデンスサービスは
ネットワーク利用内容を明らかにし
ネットワーク帯域が妥当かの証拠（エビデンス）を
明確にします。**