ITサービスレコーダー構想

企業におけるITサービスの重要性が増し、ITサービスが止まると直ぐに企業活動に影響するようになってきました。企業が安定してITサービスを利用できるように、Network, Server , client の end to end の正常運転状況の見える化が求めらています。

自動車にドライブレコーダーが必須となってきたのと同様に、ITサービスにおいても、運転状況の把握が必要になりますので、これを具体化するITサービスレコーダー構想について、説明します。

【目次】

アイティエスコンサルティング株式会社

2026/01/16

1. 企業の情報システム部門におけるITサービスの課題

企業の情報システム部門の方は、少数で、幅広い業務を担当され、エンドユーザ様の問合せ、申告・クレームの対応で、非常に苦労をされています。
以下のような例があります。

（1）コロナでWEB会議が増えかなりの帯域を利用していると考えているが、実態が分からない。

（2）WEB会議で使い勝手が悪い等の苦情があるが、どこが悪いか分からない。

（3）ネットワーク全体で課題があるのかないのか、うまく利用できているかが分からず、
問合せがある度に、調査を行っている。

（4）ある機器が突然、多くのパケットを送信し始めるケースがありましたが、実態が判明するまで、
数カ月を要した。

（5）エンドユーザ様から（情報システム担当に）
『処理が遅い』の問合せがあるが、状況が分からないため明確に回答できない。

（6）潜在故障を、トラブルの前に発見したい。

（7）ベンダ、キャリアに問合せをしても、サーバーは問題なし、ネットワークは問題なしと個々の部分では問題なしの回答を得るが、通しでは利用できない、利用に問題があることがある。

2. ITサービスレコーダーに求められるもの

ITサービスレコーダーは、
ITインフラが問題なく利用できているか、できていないかをリアルタイムで把握できる仕組み
を提供し、ITインフラの安定した運用を支援します。

必要となる要素（機能）
（1）ping試験、port試験、http試験、https 試験等の基本的な監視ができること

（2）ITインフラ全体を網羅的に把握できるように、ITインフラ全体の試験を薄く、軽く行うことができること

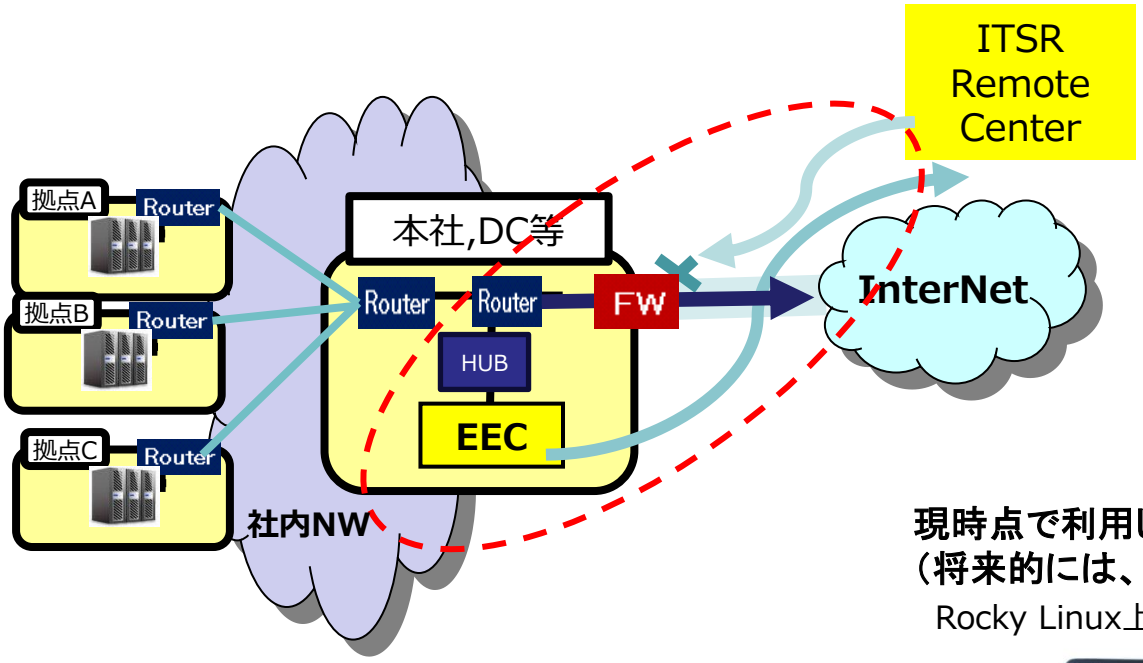
（3）各種機器からのトラフィック情報を snmp で入手できること
　前提：snmp のデータの取得は、switch, router 等の機器で事前の設定が必要です。

（4）パケットキャプチャーデータをリアルタイムで検索ができること
　前提::パケットキャプチャーを行うためには、事前に身ラポートの設定が必要です。

（5）ITサービスレコーダーとCenter間でコラボレーションが可能なこと
　この機能を利用することにより、カスタマイズ試験等　新規に調査項目を追加することが可能となります。

ITサービスレコーダーは、
情報収集機器として、現場にEEC（End to End Checker） を設置します。
及び、ITSR Remote Center（クラウド）により構成されます。

現場には、情報収集機器として、EEC（End to End Checker） を設置します。
EECは、ITSR Remote Center とセキュアにコラボレーションを取ります。



ITSR Remote Centerは、
特定のｸﾞﾛｰﾊﾞﾙIPの通信のみ許可
必要最小限のport通信の許可
Basic認証　を加え、
セキュアなコラボレーションを実現しています。

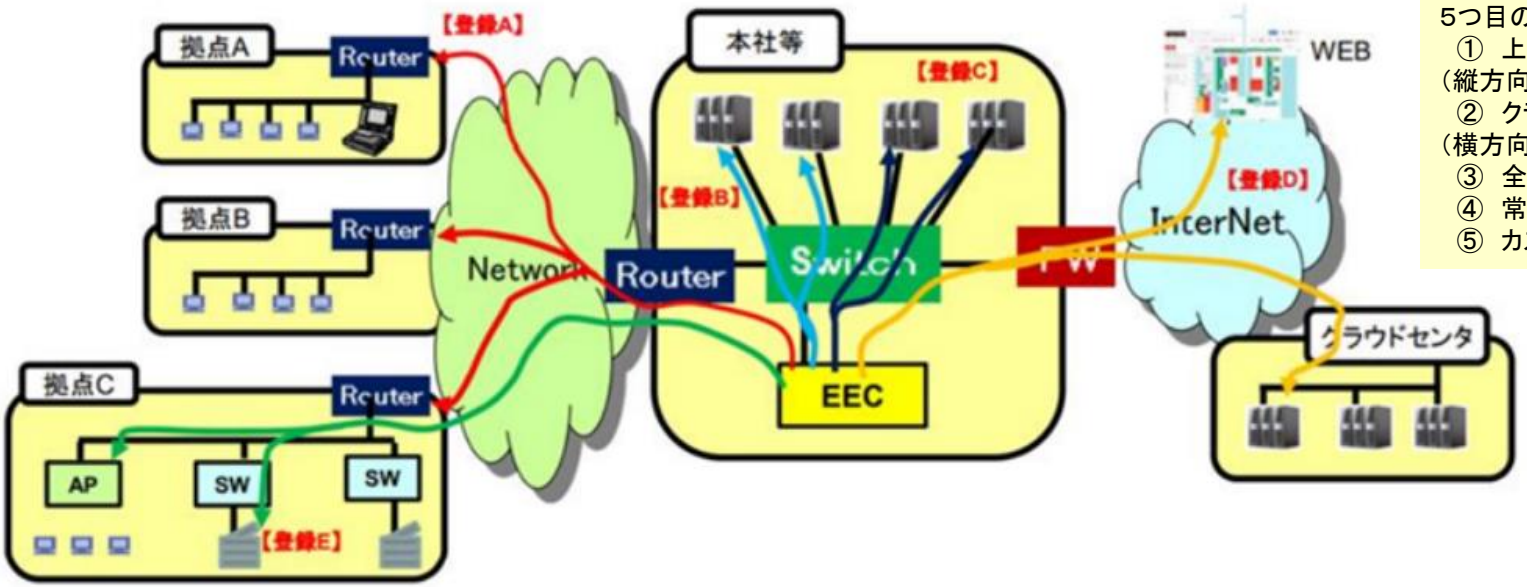
現時点で利用しているEECの外観
（将来的には、専用Box化も検討）

Rocky Linux上に　専用アプリ

(1) 電源ケーブル
(2) eth0 （NotePC内蔵LANケーブル差込口）　⇒ ミラーポートに接続
(3) eth1 (USBポートに差したUSB_LANケーブル) ⇒ LANポートに接続

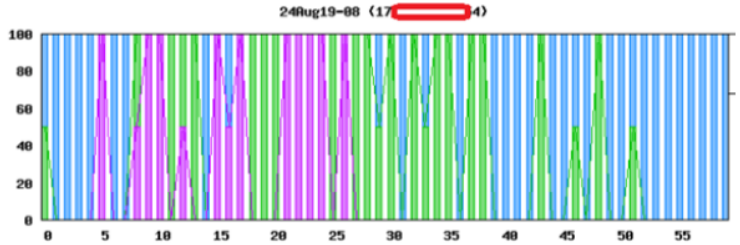
4. EEC（End to End Checker）の機能

（1）ping試験、port試験、http試験、https 試験等の基本的な監視ができること
（2）ITインフラ全体を網羅的に把握できるように、ITインフラ全体の試験を薄く、軽く行うことができること



「保守・運用サービスの
5つ目のポイント
① 上位から
（縦方向のend-to-end軸）の試験
② クライアントからサーバまで
（横方向のend-to-end軸）の試験
③ 全装置（規模軸）の試験
④ 常時監視（時間軸）
⑤ カスタマイズ試験

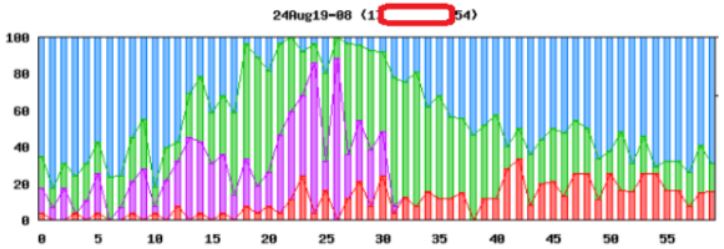
あるお客様の例
2024/08/19(月) 08時台 約１分に１回の試験



１分間に１回程度の試験では、該当の分の試験が遅いと、100%遅いの表示になります。

凡例　青：速い、緑：少し遅い、紫：遅い、赤：timeout　の 100%表示

2024/08/19(月) 08時台 試験間隔を短くした場合



試験間隔を短くすると遅延の細かい分単位の識別が可能です。
この例では、１分間に１回の試験では分からなかった timeout の状況も明らかになっています。

ITインフラを網羅的に試験を行い、全体の把握を行います。
試験間隔は、最低 1秒に 1回行うことができ詳細の状況の把握ができます。（上のグラフは、1分毎、1秒毎の試験例）

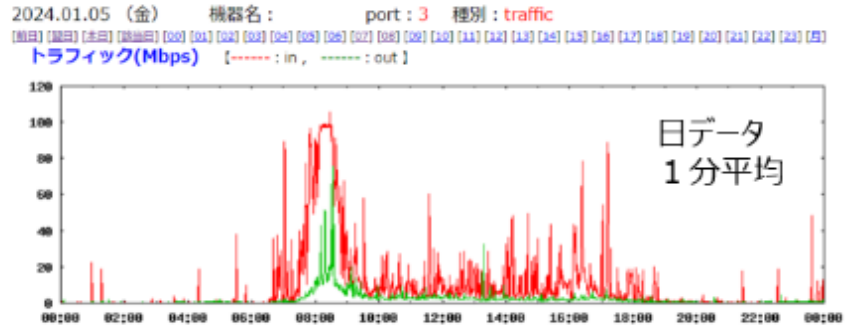
4. EEC（End to End Checker）の機能

（3）各種機器からのトラフィック情報を snmp で入手できること

前提：snmp のデータの取得は、switch, router 等の機器で事前の設定が必要です。

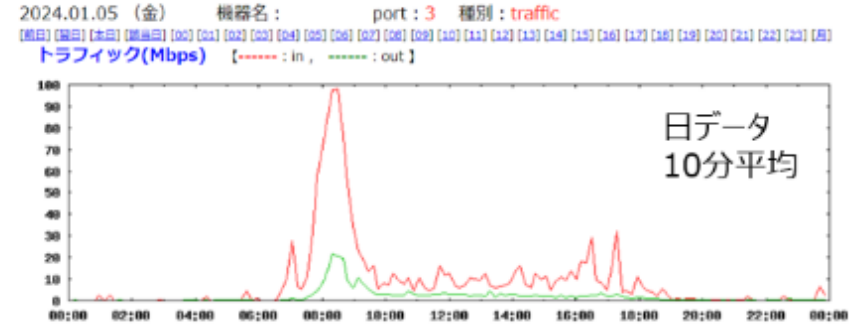
5分平均、10分平均のトラフィックデータでは、実態を把握できない場合があります。

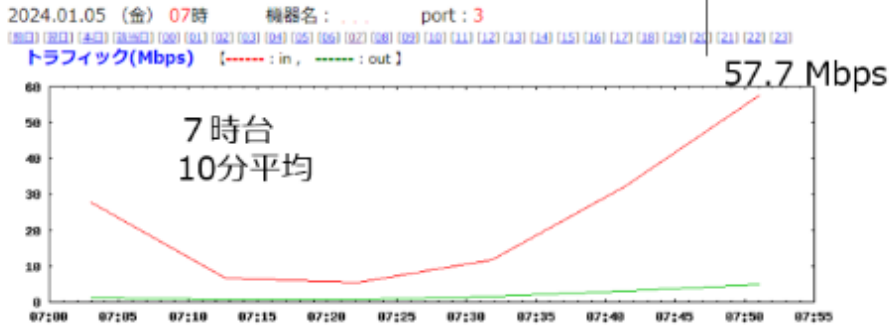
EECでは、試験間隔（平均）を自由に設定できますので、1分平均のトラフィックデータや、30秒平均のトラフィックデータも取得が可能です。



5分平均で、24%増し

1分平均で、67%増し





4. EEC(End to End Checker)の機能

(4) パケットキャプチャーデータをリアルタイムで検索ができること
　前提::パケットキャプチャーを行うためには、事前に身ラポートの設定が必要です。
・**大量にパケットを送出している機器があれば、直ぐにその機器を特定することができます。**
・現時点で、ファイルサーバーにアクセスしている機器を特定することができます。
　ある方が大量にコピーを行い(何Gbyteも)、他のお客様が利用しづらい時に、大量コピーの機器を特定することができます。

検索例
パケット時間帯:
2023-01-10 09:38:50 ～ 09:40:32
【 1 分 42 秒 】

出力内容　　:
発IP　着IP　発プロトコル　着プロトコル
の検索結果を以下に示します。

2023-01-10 09:40:32 ごろの検索結果で、
まさにこの時間帯に通信を行っている
パケットの状況です。
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

（4）パケットキャプチャーデータの分析　packet 推移のグラフ

EECでは、パケットキャプチャーを連続して取得することをお勧めしています。

週明けの月曜日（月曜日が祝日の場合は火曜日）にトラフィックが増加することが多いため、EECでは、Defaultで、この日に snap shot（パケットキャプチャーのデータの保管）を実施し、packet推移のグラフを作成することにしています（自動化処理）。
以下の例は、あるお客様の 2024.9.2（火）の packet推移のグラフです。

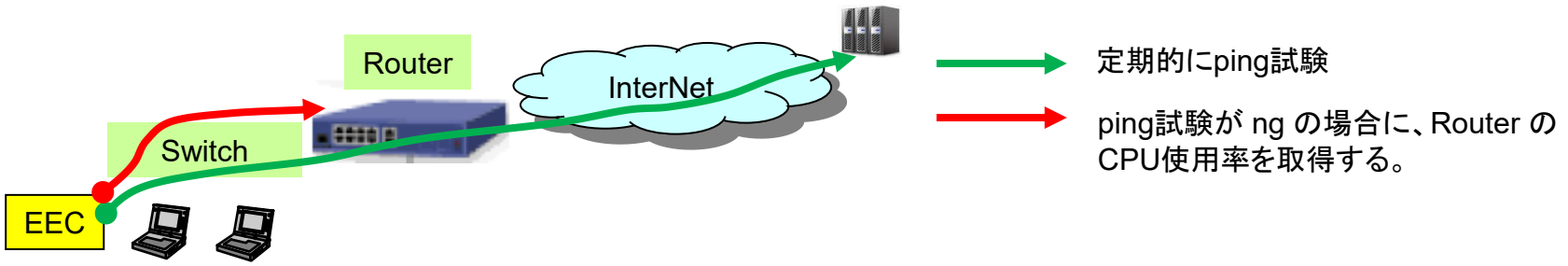
連続取得している過去のパケットデータ 5世代＋0世代（現在取得中）の全パケットデータについて、パケット数の多い TOP 10 の機器について、パケット数の推移のグラフです。

（5）ITサービスレコーダーとCenter間でコラボレーションが可能なこと
　この機能を利用することにより、カスタマイズ試験等　新規に調査項目を追加することが可能となります。

トラブルの発生時に、通常は、Router や Switch のコンソール画面より、また、機器に login をして、
show log 等のコマンドを入力して調べることが多くなっていますが、
トラブルがいち発生するか分からない場合に、調査のために、保守員が待機するのは現実的ではありません。

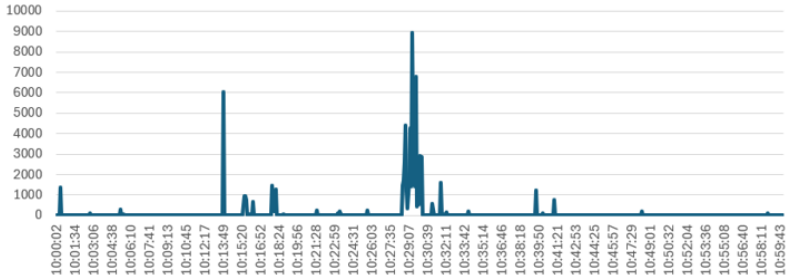
トラブルの原因を究明するには、より深い、機械的な試験、データの入手が有効です。
これを実現するのが、カスタマイズ試験です。

例1　ある機器への ping 試験が発生した時に、 RouterのCPU使用率を　snmp を用いて取得する。

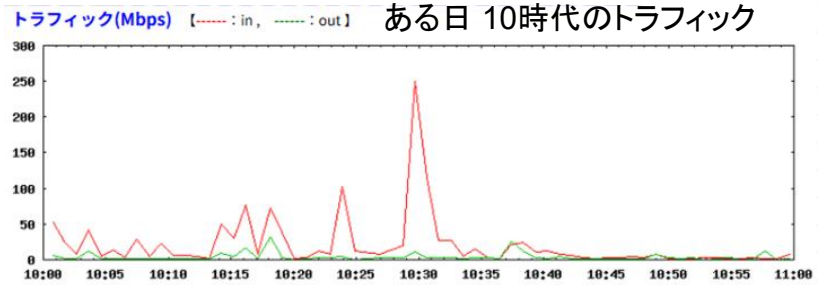


例2　トラブルが発生するため、一時的に　短い間隔で　Router 等の 廃棄packet を取得する。
　以下の例では、トラフィック増に相関して廃棄packetが増えていることが分かります。

ある日 10時代の 廃棄packet数



ある日 10時代のトラフィック



本事例は、まだ、ITサービスレコーダー構想が無かった時に、トラブル解決まで時間がかかった例です。
問題の解決まで、現場に何度も足を運び、3カ月の時間を要しました。
ITサービスレコーダー構想があれば、パケットのリアルタイム検索により、直ぐに原因を発見することが可能です。

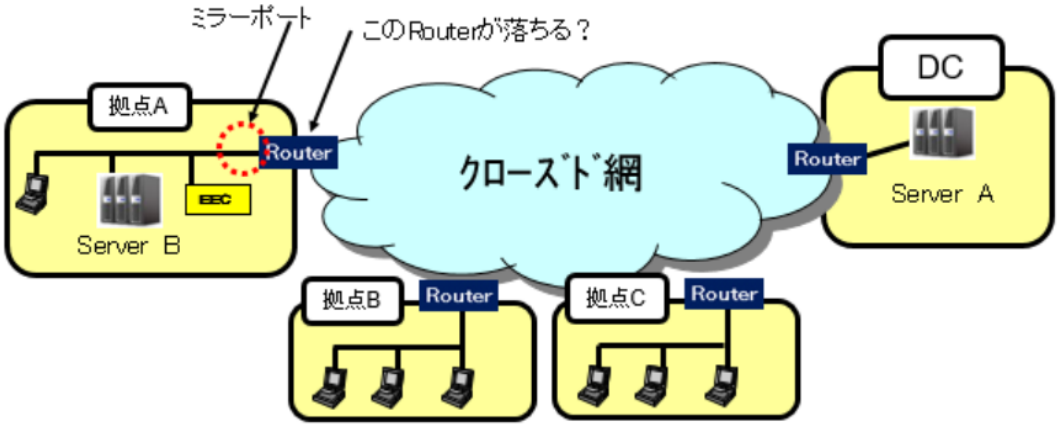
【事例】 帯域に余裕があるのにRouterが落ちる
（1）事象の概要
　毎月、決まった日にデータセンターにあるサーバのアプリケーションが使えなくなりました。レスポンスが遅いので、Routerの電源をoff／onにすると復旧しました。
・回線の帯域を調べましたが、帯域をほとんど使用していなく、回線の圧迫はありませんでした。
・Routerのダウンを表すアラームも発生しておらず、電源をoffした時点で、回線ダウンアラームが発生しました。
　原因が分からず、該当日になると、情報システム部員が待機し、電源のoff／onを実施する必要があり、その作業の間にアプリケーションが使えないと言う大きな問題でした。

【原因の要約】
　あるサーバが、WindowsUPdateの後（月１回）のReboot後に大量の端末とのアクセスで接続エラーが発生し、このサーバが不要な信号パケットを多量に発生しました。Routerは、ダウンはしていないが、この大量処理のために、pingの応答もできない状態に陥り、監視装置はRouterの死活監視エラーとなり、ダウン状態とみなしてしまいました。
　まず、異常時に大量にパケットを発生するサーバの特定を行い、そのサーバと接続しているパケットキャプチャーの分析を行いました。
その結果、サーバーが多くの機器と複数のプロセスを大量に発生していることが判明し、この処理を回避することにより問題を解決しました。
　原因究明に至った事項を詳細に記述します。

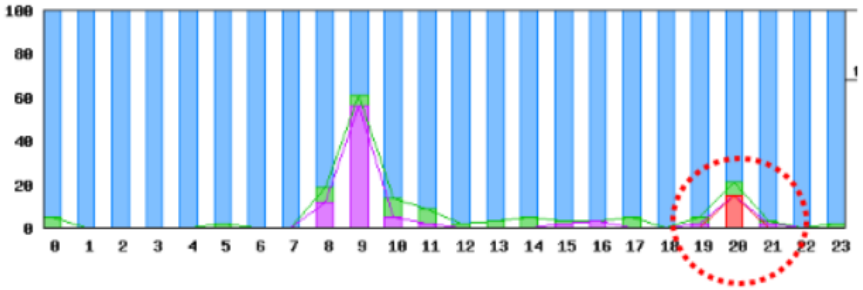
（2）システム構成

使用できなくなる拠点のRouterのパケットをキャプチャーするために、Routerの通信が取れる場所にミラーポートを作成しました。

次の図が、今回のトラブル事象の全体構成です。



トラブルが生じた時のEECの通常監視のデータを示します。




```
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
```

Routerの死活監視(ping) で timeout が発生しています。

象からみると、Router 異常、回線異常と考えがちです。

（3）パケットキャプチャー取得の工夫

パケットキャプチャーは、EEC(End to End Checker)のパケットキャプチャー機能を利用しました。
該当拠点に設置したEECに遠隔でパケットキャプチャーの起動を行いました。

また、「突発トラヒック見える化」機能を利用して、EECの監視対象拠点をダウンアラーム情報を元にパケットキャプチャーを実施し、自動的にパケットキャプチャーをすることで原因究明に役立ちました。

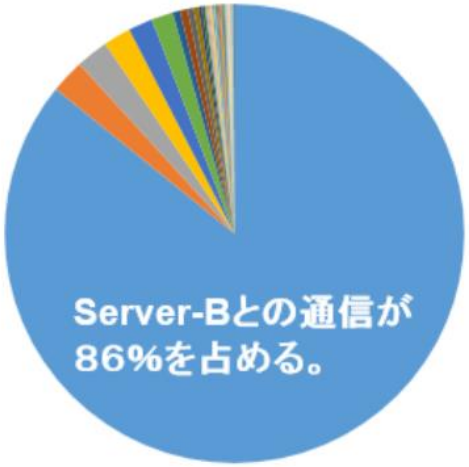
【補足】

ITサービスレコーダー構想の検討中の事象で、パケットキャプチャーの取得方法のバリエーションについては、現行機能を先行して実施しています。

（4）新たに発見されたサーバの通信

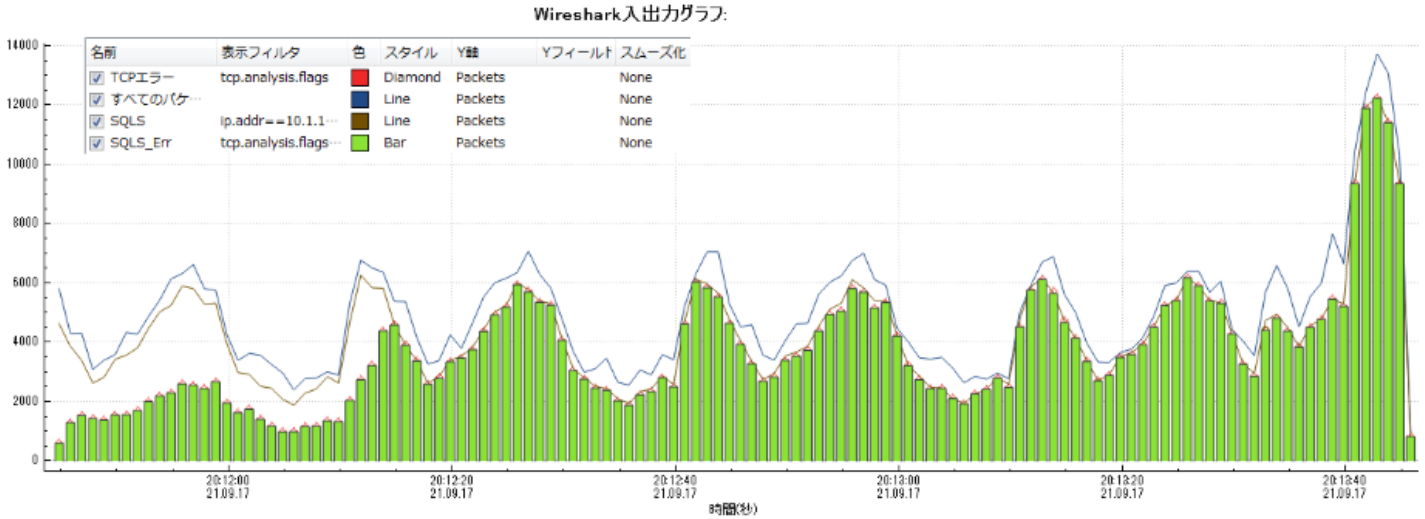
次に示しますのは、トラブル中のパケット通信の上位10のIPアドレスです。

	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



拠点Aの端末において、DC（Data Center）にあるServer-Aとの通信が遅いことが問題の起点でしたが、新たにServer-Bの通信が影響することが分かりました。
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, ... との通信であることが分かりました。

次に示しますのは、
①パケットキャプチャーの全データ、②Server-Bの通信、③全データのTCPエラー、④Server-BのTCPエラーのパケット数を示したWireSharkのグラフです。



次　Server-Bの通信のほとんどが、TCPエラーの通信であることが分かります。
エラーパケットは情報量がほとんどないため、使用帯域はごく僅かになっています。帯域には余裕があるのにServer-Bの通信のため他の通信ができない状態に陥りました。
　ここで注意が必要なのは、Routerとしては、ダウンはしていませんでした。しかしながら、ping応答ができない程、不要なパケット通信が生じてしまいました。

（5）まとめ
　今回の事例は、原因となったServer-Bが発見しにくかったことです。当初は、帯域が利用されないのにも関わらず、Routerの電源off/on を行うと一時的にサービスが回復するため、Router、もしくは回線に関係することが原因と考えられていました。
　パケットキャプチャーを行うことにより、当初考えていなかった、Serever-Bの存在が明確になり、その処理に問題があることを発見することができました。

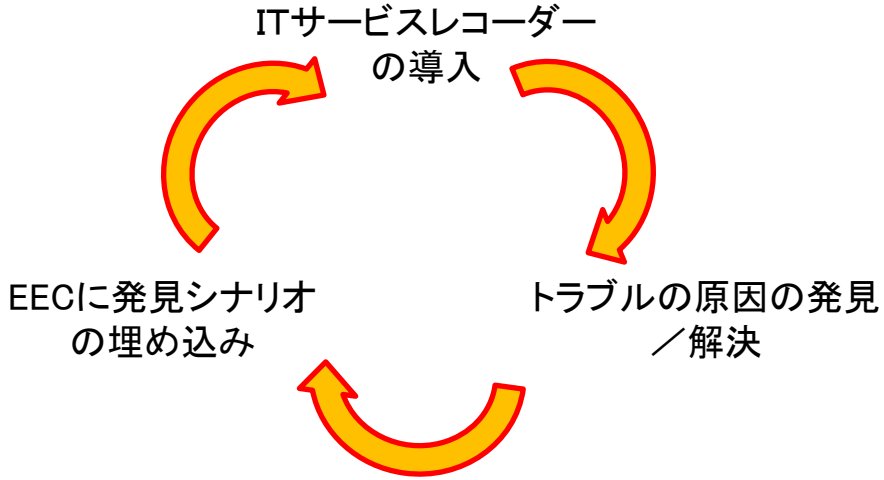
6. まとめ

ITサービスレコーダー構想について記述しました。

ITサービスは、今後も重要度が増し、安定したサービスの提供が望まれます。
安定したサービスの提供が必要ですが、
それを支える　情報システムのスキルを持った技術者の不足が顕著となり、
各企業の情報システム部門の方は、少数で過酷な業務が増えております。

このような背景で、各企業の情報システム部門の方を支援するのが、
ITサービスレコーダー構想です。

ITサービスレコーダー構想により、解決できた事象については、
トラブルの発見に至ったシナリオを　現地に設置するEEC（End to Enc Checker）に盛り込んで
いくことにより、更に、トラブルの発見が早くなるという　好循環のサイクルとなります。



ネットワークシステムの技術/運用に関して、
ITサービスレコーダー構想が、少しでもお役に立てれば幸いです。