「生成AI（LLM）を活用したパケット・Syslog分析」を大規模NWで実証してみた

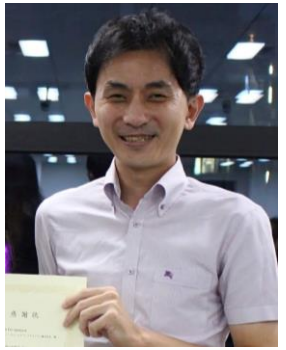
2025年8月1日

NTTアドバンステクノロジ株式会社
ソーシャルプラットフォーム・ビジネス本部 IOWNプロダクトビジネス部門 ネットワークシステム高度化担当

発表者

髙野　悠生(たかの ゆうき)

2011年入社。NGN開発・維持管理を複数担当した後、新技術開発チームに移動。
NWアクセラレータとしてのFPGA開発・システムアーキテクチャ検討の傍ら、
2019年から、Interop ShowNetのAT社コントリビュータリーダを務めています。
最近は専ら「ミニPCで動作するLLMアプリケーション開発」にハマっています。



環　大介(たまき だいすけ)

2019年入社。新技術・新製品チームに配属されました。
FPGAを活用したシステム開発業務に従事する傍ら、
HWアクセラレータのコンテナ仮想化技術などに取り組んでいます。

阿部　拓実(あべ　たくみ)

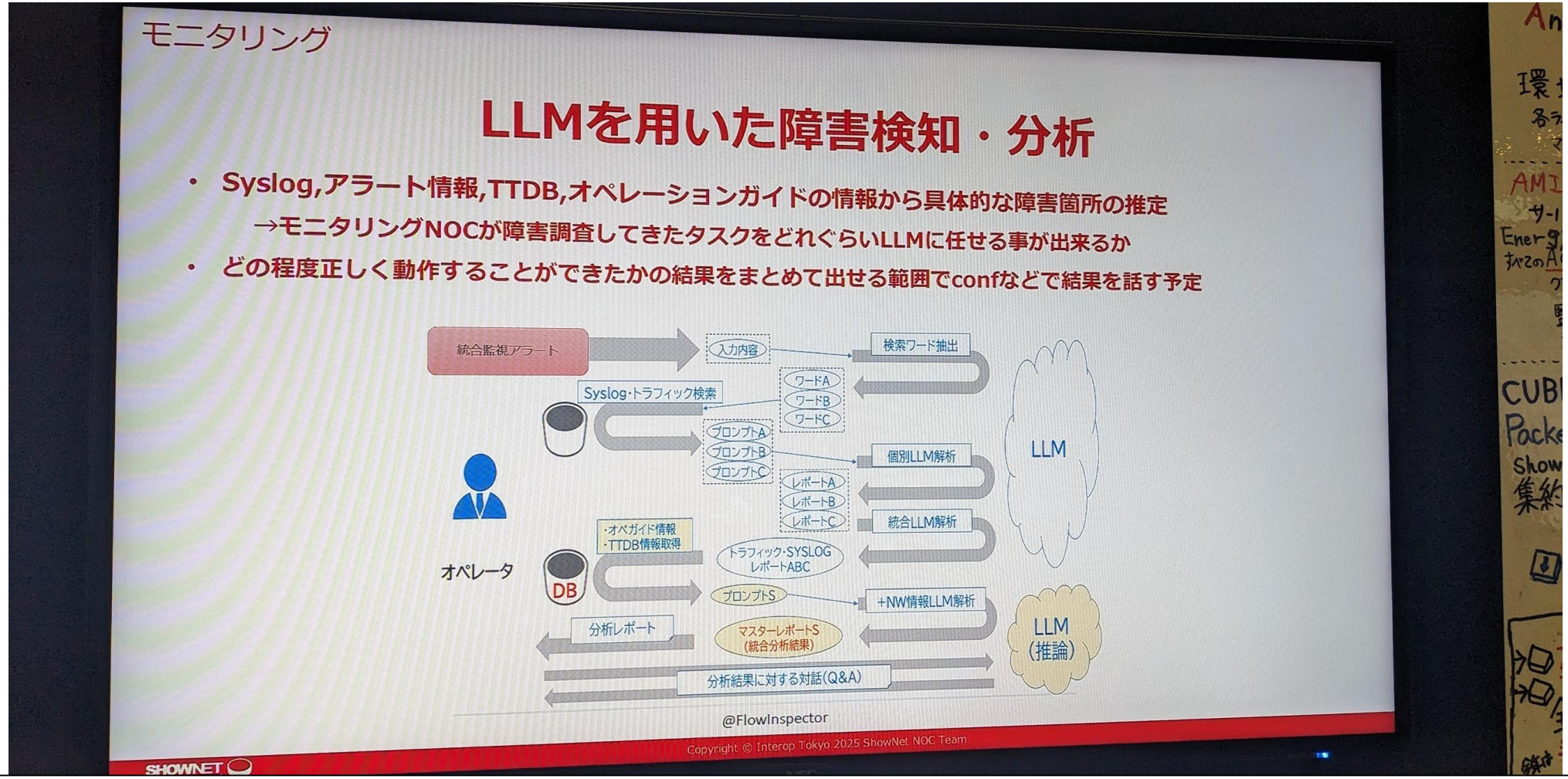
2023年入社。配属からFPGAの新技術・新製品チームの技術SEとして従事。
FPGAを用いたシステム検討や検証作業などの業務を通して日々修行中。
趣味はゲームと野球観戦(巨人推し)。※現在現地2勝-1敗

生成AI　×　パケットログ　×　ネットワーク構成

Interop Tokyo ShowNet 2025における実証実験(1)

ShowNet NOCチームメンバー作成資料「【展示会場内説明スライド】モニタリング ShowNet 2025」より引用
https://speakerdeck.com/shownet/zhan-shi-hui-chang-nei-shuo-ming-suraido-monitaringu-shownet-2025

Interop Tokyo ShowNet 2025における実証実験(2)



ShowNet NOCチームメンバー作成資料「【展示会場内説明スライド】モニタリング ShowNet 2025」より引用
https://speakerdeck.com/shownet/zhan-shi-hui-chang-nei-shuo-ming-suraido-monitaringu-shownet-2025

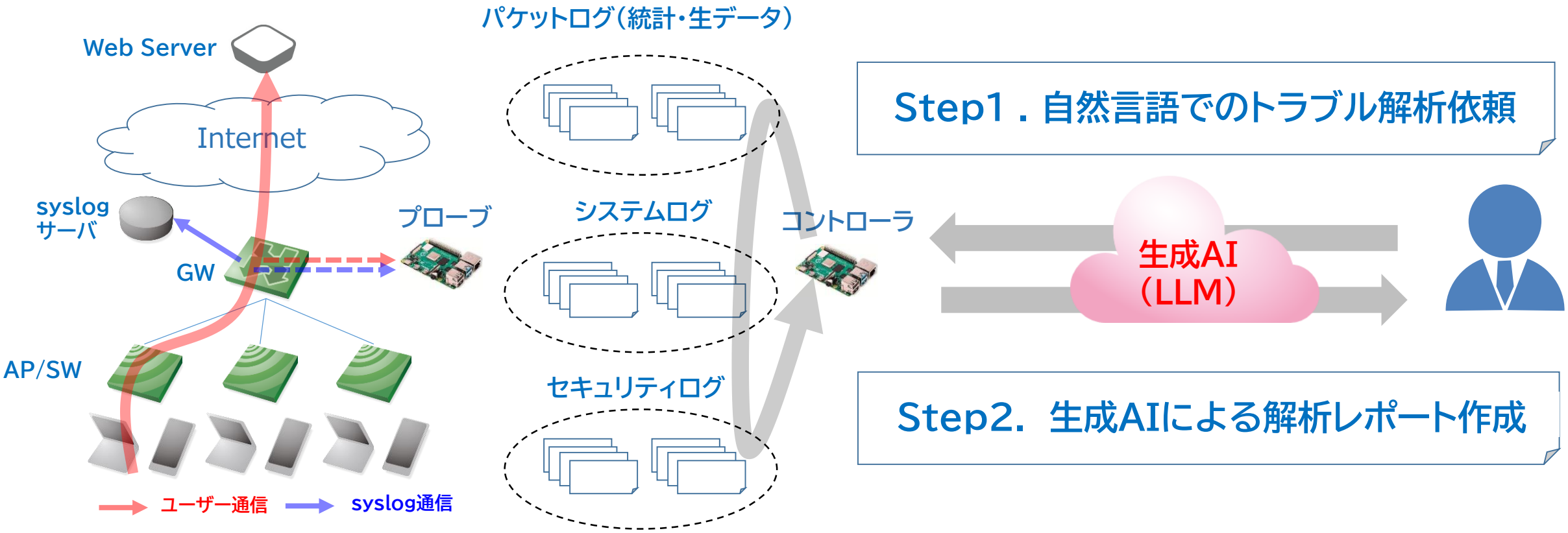
生成AI　×　パケットログ　×　ネットワーク構成

生成AI × パケットログ × ネットワーク構成

トラフィック・Syslog解析システムのコンセプト

Generative AI Packet AnalyzeR（GAIPAR）

「ネットワークのトラブルシューティング」を簡易に実現するシステム



Step1．自然言語でのトラブル解析依頼

Step2．生成AIによる解析レポート作成

オペレータはどうやって「障害原因」を特定するか？

例：「特定サービスにwebアクセスできない」というユーザ申告があったら？

SYSLOG・統計情報

パケットキャプチャ（通信ログ）

サービスポートは解放されているか？
RSTを応答していないか？
ステータスコードは何が返却されているか？

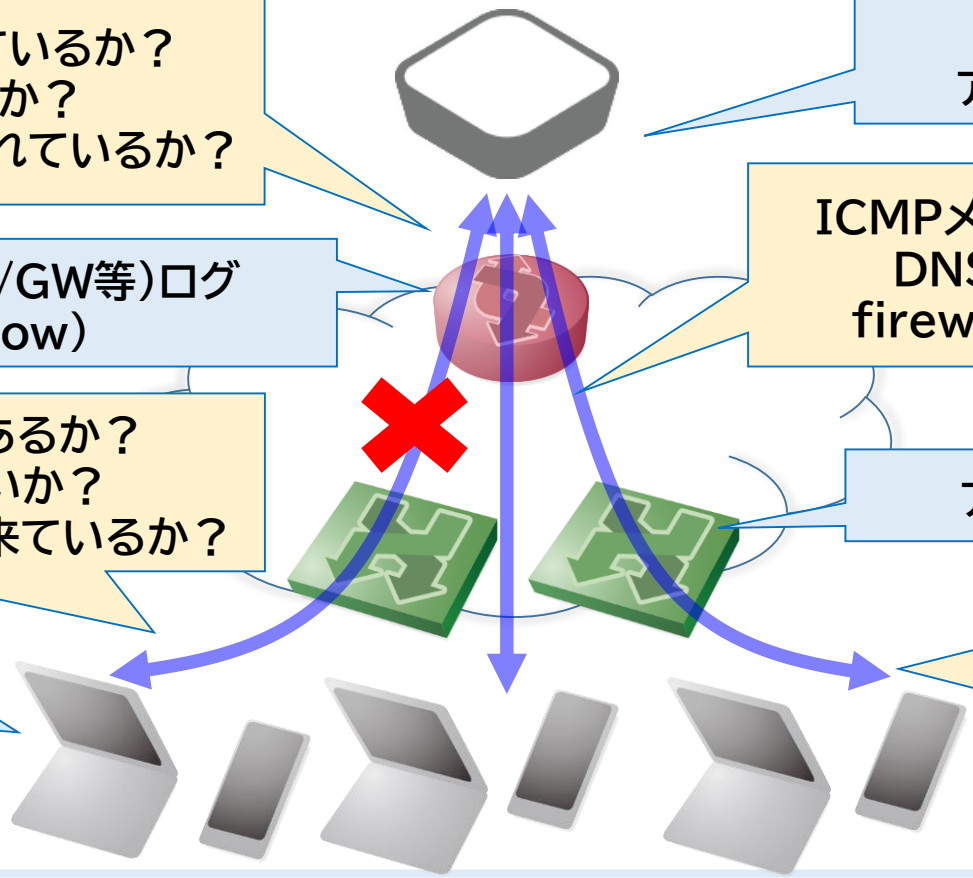
OS/OSSのログ
アプリケーションログ

ネットワーク装置（ルータ/GW等）ログ
統計情報（Netflow）

ICMPメッセージが返却されていないか？
DNSクエリが解決できているか？
firewallでフィルタされていないか？

SYNに対するSYN+ACKがあるか？
TCP再送を繰り返していないか？
アプリケーションパケットは送信出来ているか？

アクセス装置（AP/SW等）ログ

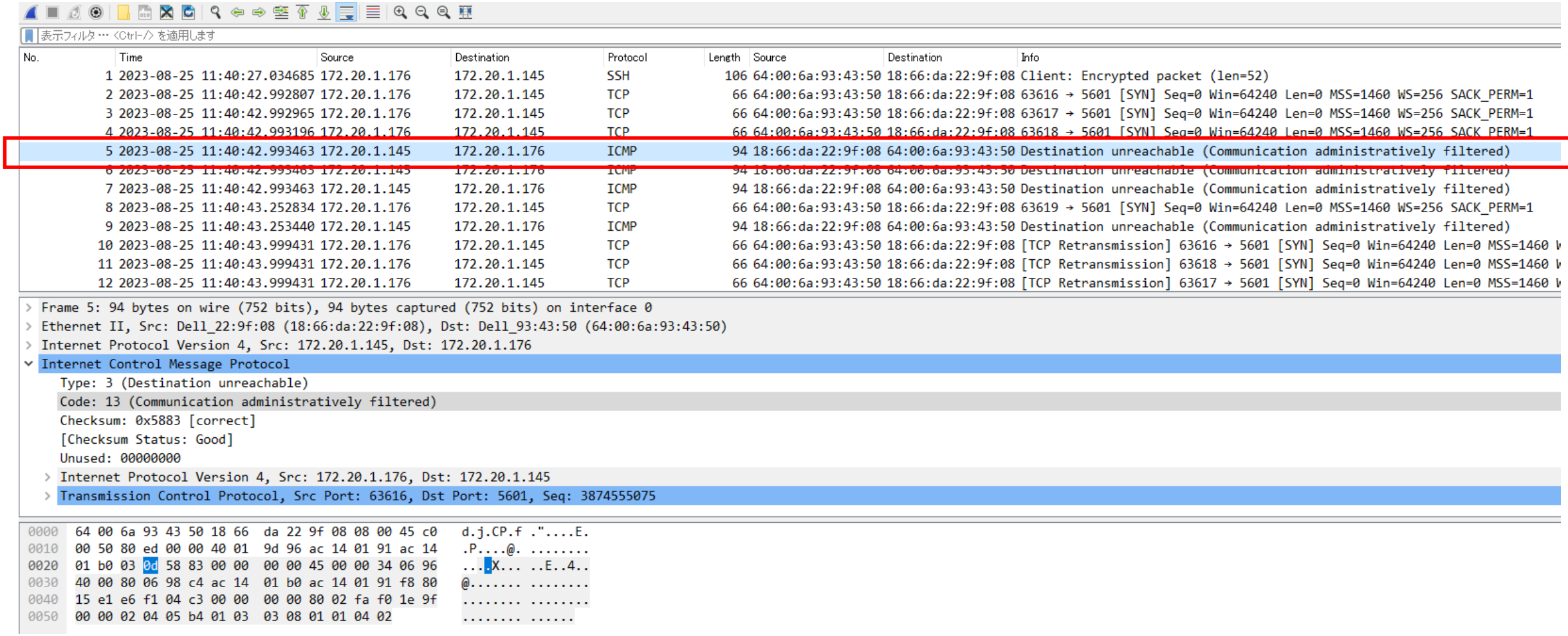


クライアント端末ログ
問題時の画面キャプチャ

他端末からの通信は正常か？
ARPが解決出来ているか？
アドレス重複が発生していないか？

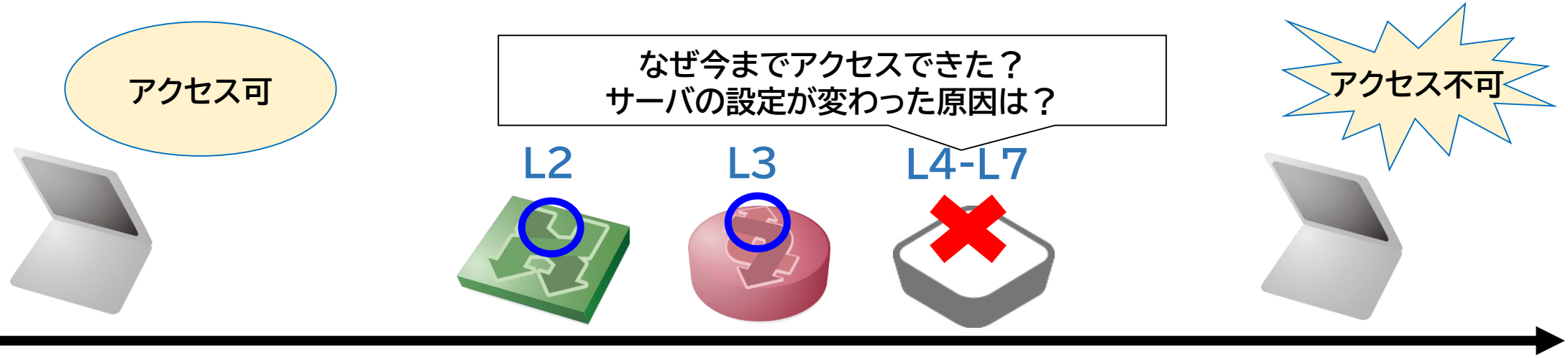
サービスアクセス不可の例

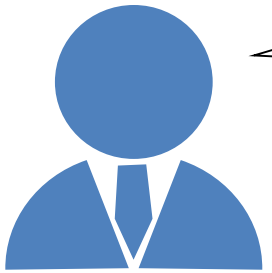
例 ： アプリケーション搭載Linuxサーバのfirewall設定漏れ



現実のオペレーションはもっと大変

障害解析から問題特定・解決に至る行程は更に複雑であり、
オペレータは「時系列に沿った今回のお話(ストーリー)」を語らなければならない





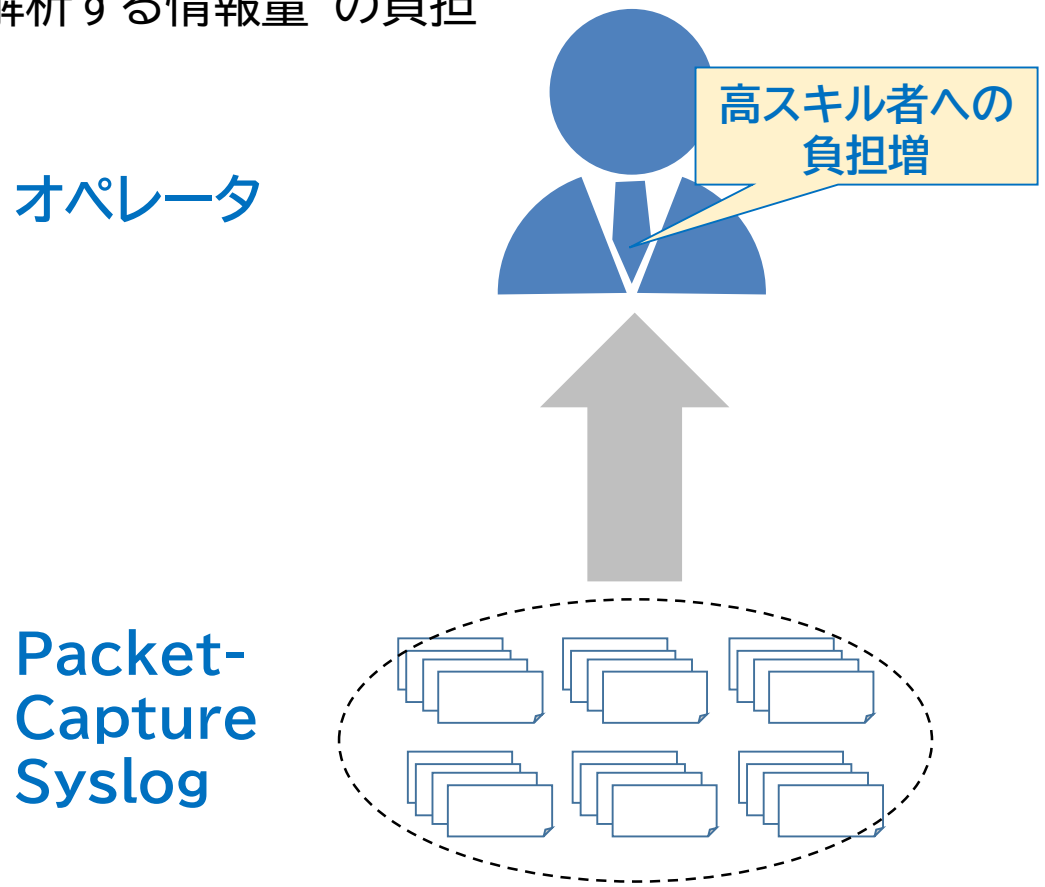
・14時半から15時の間にサービスアクセス不可となった【外部情報】
・該当時間中にサービス断・NW断を示すログ情報はなかった 【SYSLOG情報】
・ICMP Port Unreachableが返却されていた 【パケットキャプチャ情報】
⇒ アクセス不可の原因はFWの設定漏れだが、なぜいきなり？

・設定変更作業が14時半に入っていた 【SYSLOG情報＋スケジュール情報】
・FWサービスを再起動する工程があった 【SYSLOG情報＋チャット情報】
⇒ サービス再起動時、設定保存漏れでフィルタが揮発してしまっていた(手順誤り)

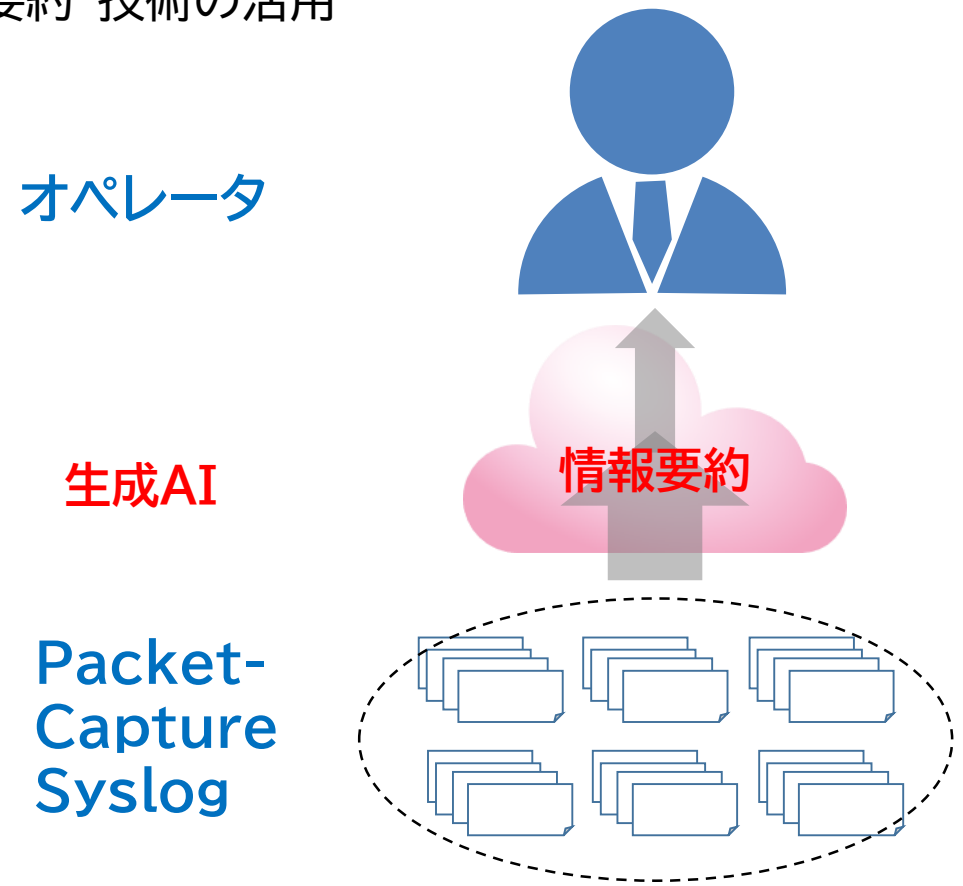
ネットワークオペレーションの課題と解決

生成AI技術の得意とする”情報要約”技術の活用により、
パケット解析・ログ解析の原因特定にかかる分析コストの低減を図ることが目的

“解析する情報量”の負担



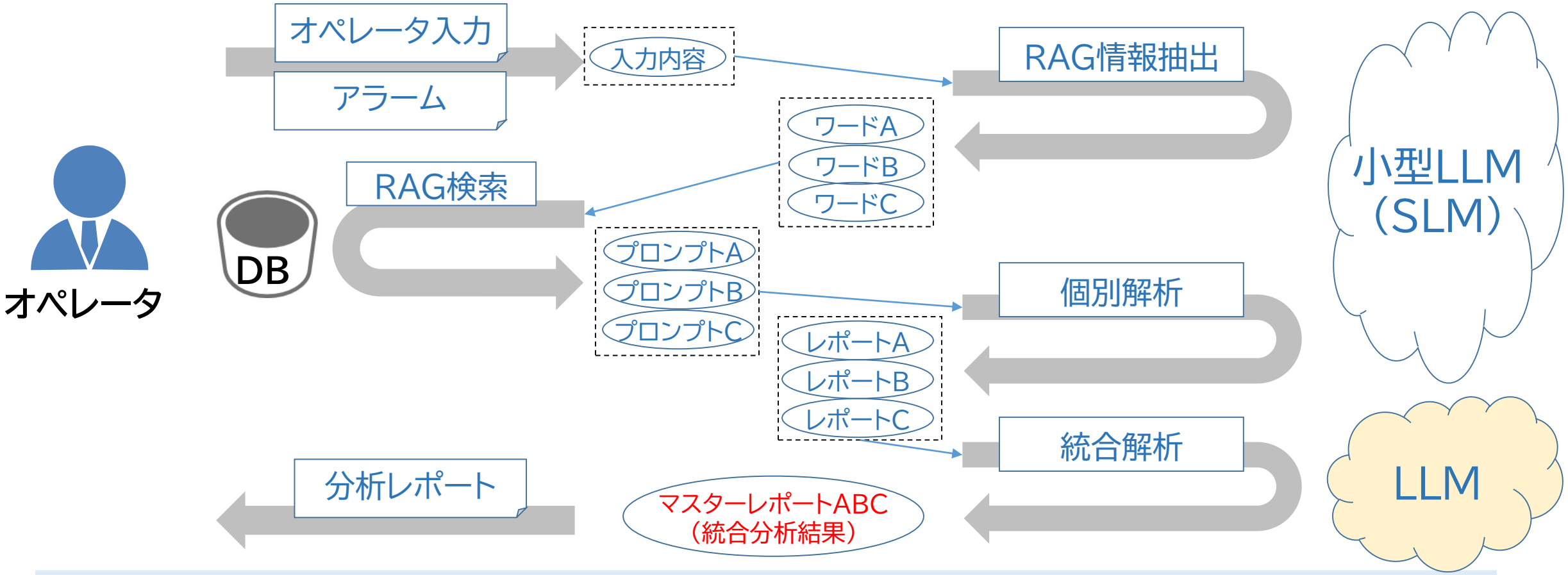
“要約”技術の活用



生成AI × パケットログ × ネットワーク構成

①階層型パケットログ（キャプチャ・Syslog）解析の流れ

Step1. オペレータが入力した文章から「解析に必要となる分析キーワード」を抽出
Step2. トークン数を調整しながら分析キーワード単位の「個別分析レポート」を発行
Step3. 個別解析レポートを集約し「統合分析レポート」を発行



②LLM向けネットワーク解析プロンプトの作成

当日発表資料・アーカイブでご説明します。

パケット・SYSLOGをLLM解析できるプロンプトとは？

当日発表資料・アーカイブでご説明します。

コンテキストのフィルタリング(1)

当日発表資料・アーカイブでご説明します。

コンテキストのフィルタリング（2）

当日発表資料・アーカイブでご説明します。

解析するパケットデータ量の削減

当日発表資料・アーカイブでご説明します。

通信フローへのSYSLOG情報の挿入

当日発表資料・アーカイブでご説明します。

LLM利用を運用するためのコストとは？

「LLMを利用したネットワークオペレーション」は技術が先行しがち
⇒ 実適用に許容される”コスト”とは？
⇒ LLM利用による削減コスト ＞ LLM運用コストを期待したい

① イニシャルコスト
共通 ： LLMオペレーション向けサーバの新規購入費

② ランニングコスト
外部LLM利用 ：OpenAI,Claudeを始めとする外部API
ローカルLLM利用 ： 基本的にはなし(本当に…？)

「イニシャルコストを下げて使いやすくする」提案

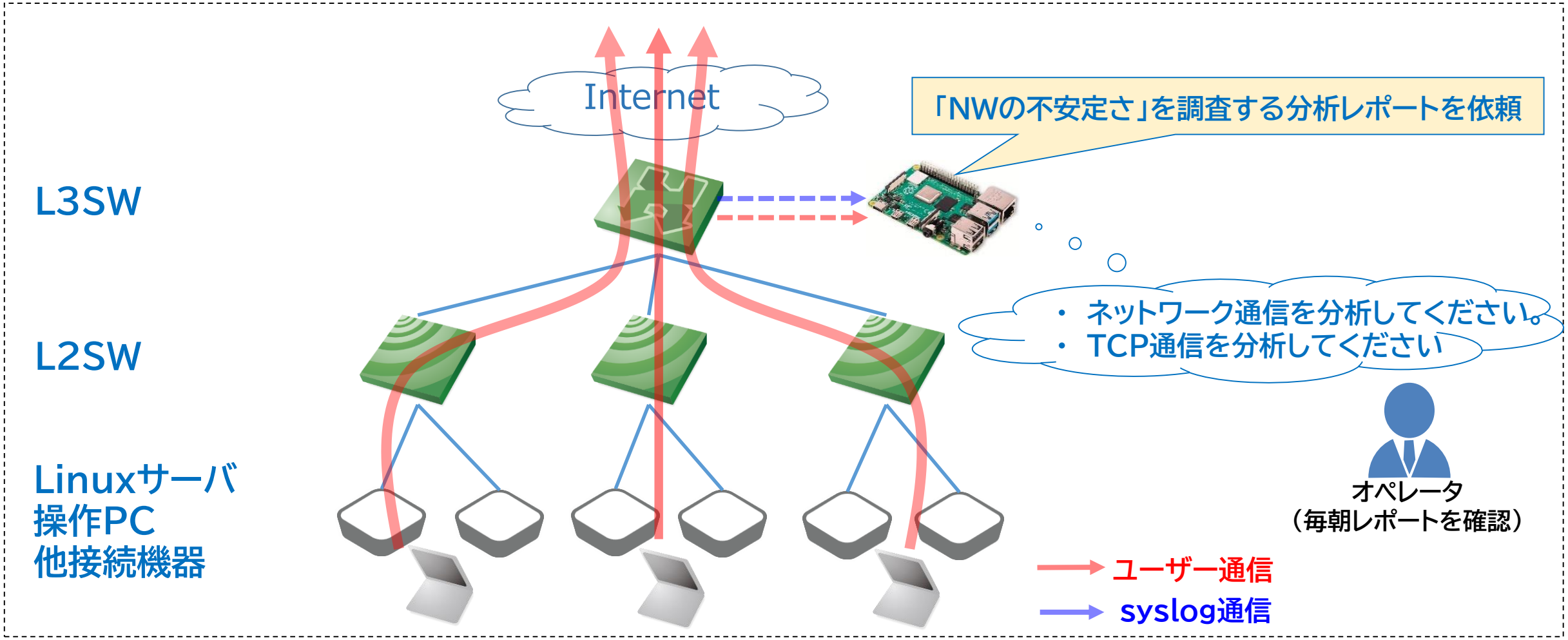
当日発表資料・アーカイブでご説明します。

「ローカルLLM利用」は運用コスト削減に繋がるか？

当日発表資料・アーカイブでご説明します。

【分析例】LLMを用いたネットワーク分析レポート

例 ：「NWの不安定さ」を調査するネットワーク・サーバ通信の分析レポート



【分析例】ネットワーク分析依頼の入力

分析チャットから問合せしたい内容を入力し、パケットログを検索

分析したい概要を入力してください。

2025年6月22日のネットワーク通信について、分析してください。

- ["tcp","dns","udp","dhcp","http","arp","icmp","ntp","mac","snmp","syslog","down","err","warn","fail"]
- 20250622 0000
- 20250622 2359

【分析例】分析されるキーワードの例(1)

（ネットワークが不安定なので、）
2025年6月22日のネットワーク通信を分析してください。

抽出キーワード	キーワードから分かること
tcp	TCP通信で過剰なSYN・再送・バッファ不足エラー等を示す出力がないか
dns	DNS解決エラー等が発生していないか
udp	UDP通信が出来ているか、パケットに破損がないか
dhcp	DHCP解決が正常に行われているか
http(s)	HTTPアクセスが正常に行われているか(500エラー等が返ってきていないか)
icmp	到達不能(unreachable)メッセージが返却されていないか
arp	ストームやIP競合が発生していないか
snmp	NWエラーを示すsnmptrapが発行されていないか
syslog	NWエラーを示すsyslogメッセージが発行されていないか
down / warn / fail	一般的なエラーメッセージが含まれるパケットログが存在していないか

【分析例】分析されるキーワードの例(2)

（ネットワークが不安定なので、）
tcp通信を分析してください。

抽出キーワード	キーワードから分かること
SYN	SYNの数やSYN Flood等の問題が発生していないか
RST	サーバのアプリ異常やポート閉塞が発生していないか
retransmission	TCP通信の再送が発生していないか
Duplicate ACK	連続してDup ACKが発生していないか　※輻輳時によく発生
unreachable	ルーティングミス、ACL、MTU超過が発生していないか
Window Zero	アプリのTCPバッファに問題が発生していないか
NXDOMAIN	FQDNの設定誤り、プロキシ異常等が発生していないか
Malformed	パケットが破損していないか
checksum	パケットのチェックサムエラーが発生していないか

【分析例】ネットワーク分析レポートの出力例(1)

「キーワード単位の個別レポート内容」に対し、再度統合分析が実行される

1. 個別レポート情報

(1) 個別分析でユーザーが入力したプロンプト

- 「2025年6月22日のネットワーク通信について分析」

ユーザー入力内容

ユーザー入力内容に合わせて
期間内のパケットログを分析

(2) 個別分析で検索したkeyword内容、ヒット件数、時間

keyword	ヒット件数	ログ時間範囲
tcp	5,204	2025-06-21 23:43:08 〜 2025-06-22 02:03:22
dns	96	2025-06-22 00:22:31 〜 2025-06-22 22:25:23
udp	0	2025-06-22日（詳細時間不明）
dhcp	42,249	2025-06-21 23:42:40 〜 2025-06-21 23:59:16
http	14	2025-06-22 01:15:17 〜 2025-06-22 21:28:58
arp	148,437	2025-06-21 23:42:39 〜 2025-06-21 23:47:10
icmp	334	2025-06-22 00:12:35 〜 2025-06-22 22:50:47
ntp	1,968	2025-06-21 23:48:15 〜 2025-06-22 05:54:46
mac	0	2025-06-22日（24時間分）
snmp	0	2025-06-22日（24時間分）
syslog	0	2025-06-22日（詳細時間不明）
down	0	2025-06-22日（詳細時間不明）
err	12	2025-06-22 00:00:00 〜 2025-06-22 23:59:59
warn	0	2025-06-22日
fail	0	2025-06-22日

【分析例】ネットワーク分析レポートの出力例(2)

問題推測は「パケットログから推測できる時系列仮説」を含め、原因の特定に寄与

(7) 分析結果まとめ

- **ARPリクエストの多発**は、[redacted]245のホストがネットワーク上で応答していないことが主因であり、物理障害（NIC故障、ケーブル断線、スイッチポート障害）または論理障害（VLAN設定ミス、ARPテーブル不整合、セキュリティ設定誤り等）が考えられる。
- **169.254.169.254宛のARPリクエスト**は、DHCP障害やネットワーク分断の兆候であり、[redacted]のネットワーク設定やDHCPサーバの状態確認が必要。
- **flow統計情報**から、ブロードキャスト/マルチキャストトラフィックが多く、ARPリクエストの多発がネットワーク全体の遅延や不安定化を助長している可能性が高い。
- **次のアクション**として、[redacted].245の物理・論理両面での切り分け、関連ホストのネットワーク設定・ログ確認、スイッチ・ルータのARP/MACテーブル確認、ブロードキャストトラフィックの監視強化を推奨する。
- 物理障害が否定された場合は、ネットワーク機器の設定（ARPキャッシュタイムアウト、Dynamic ARP Inspection等）やVLAN構成、L2ループの有無を重点的に調査すること。

時系列仮説立案：

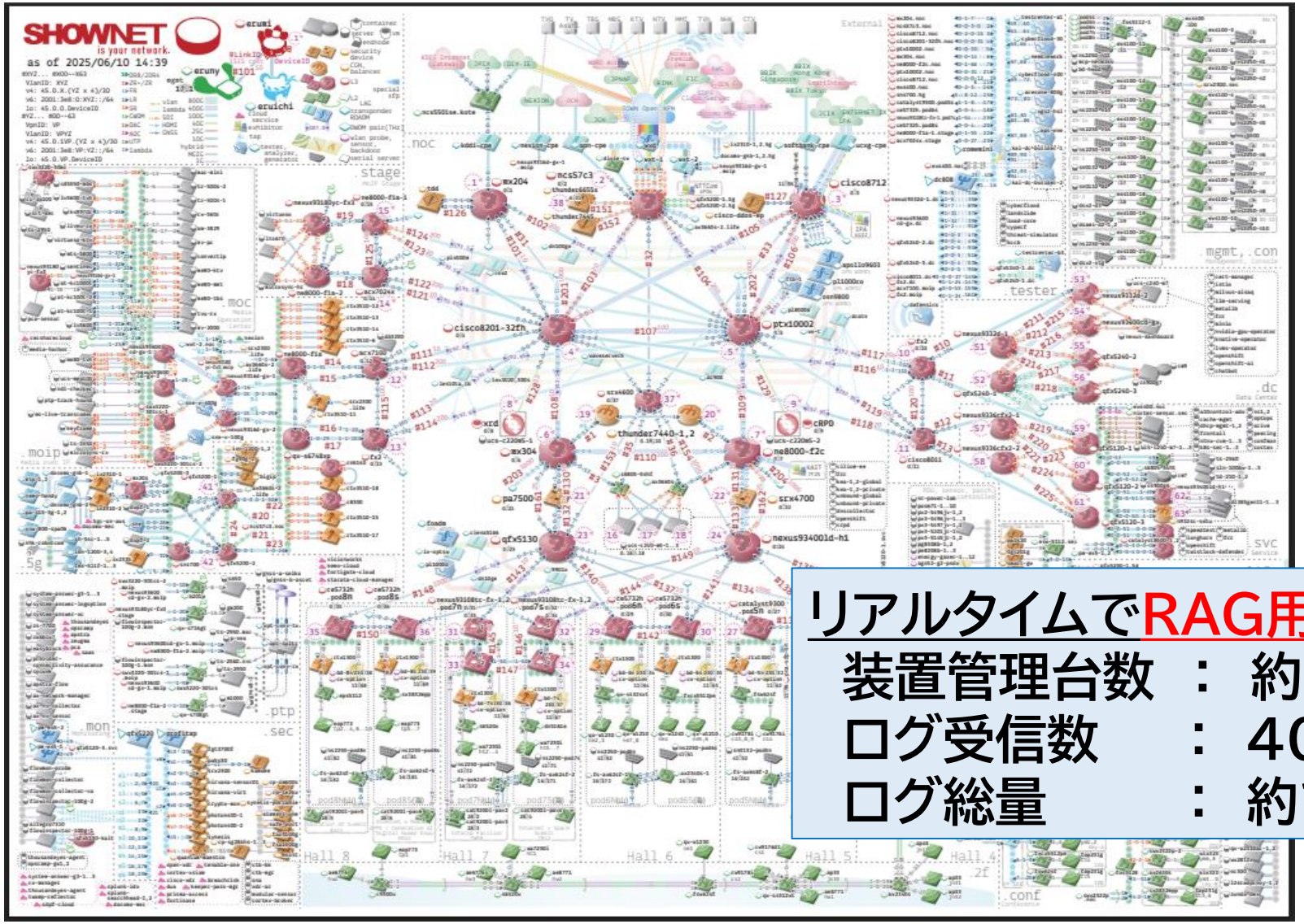
時系列で仮説を立案

- 23:42:39以降、複数ホストから[redacted].245宛のARPリクエストが継続的に発生しているが、ARP応答が返っていない。
- これによりARPテーブルが更新されず、通信が成立しないため、各ホストがARPリクエストを再送し続けている。
- 同時に、169.254.169.254宛のARPリクエストも発生しており、DHCP障害やネットワーク分断の兆候が見られる。
- ブロードキャストトラフィックの増加がネットワーク全体の遅延・不安定化を助長している。

「ネットワークの不安定さ」が
ブロードキャストにあることを推測

生成AI　×　パケットログ　×　ネットワーク構成

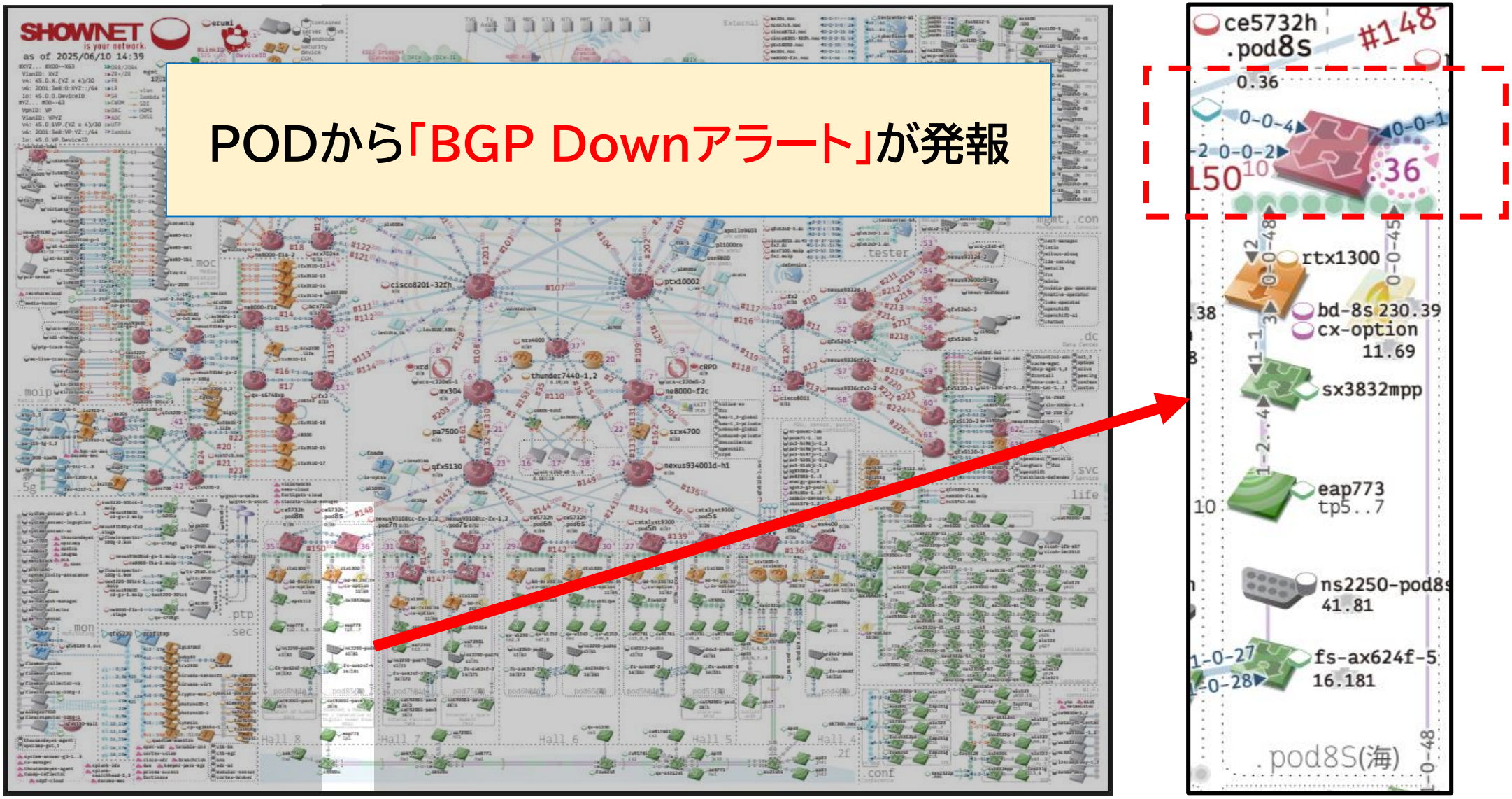
ShowNetネットワーク図



リアルタイムでRAG用ログデータを受信

装置管理台数　：　約400台
ログ受信数　　：　4000～5000[msg/sec]
ログ総量　　：　約1.5TB

トラブルケース



実際のトラブルシューティング内容

① PODからBGP downアラート発報を確認

② PODのログ・設定を確認
（1）BGP downの原因が”Hold Timer Expired”であること
（2）BGP対向がxx.xx.xx.xxであること
（3）直前にospf neighbor statusが一度downしてestablishしていること
（4）さらに直前にinterface 25GE0/0/1が一度downしてUpしていること
（5）interface 25GE0/0/1がアップリンク設定・状態であること

③ 上記情報から時系列で原因を推測
物理down➔ospf down➔BGP hold time expired
の順に発生し、物理downがトリガーであることを把握

④ 物理linkを被疑箇所として、モジュール・ケーブル・中継区間の切り分けにうつる

アラート発報要因 ： アップリンクの物理レイヤトラブル

ShowNetネットワーク情報カスタマイズ前(1)

※ShowNet ネットワーク情報 カスタマイズ前の状態を使用

検索

@FlowInspector mini

Generative AI Packet AnalyzeR (GAIPAR)

version 1.0.2

Markdownをダウンロード

コンフィグファイルを編集

統合分析レポート

1. 個別レポート情報

(1) 個別分析でユーザーが入力したプロンプト

- Problemin1m30s:SNMPTrapBGPBackwardTransitionHostce5732h.pod8s[redacted]Eventtime2025.06.1000:27:49SeverityAverageOpdata20250610:002749BGPBackward
  設定済み:PARENT:qfx5130.nocTriggerdescription

(2) 個別分析で検索したkeyword内容、ヒット件数、時間

Keyword	ヒット件数	時間範囲
[redacted]	98	2025年6月10日 00:19:44 - 00:26:43
ce5732h.pod8s	17	2025年6月10日 00:21:28 - 00:27:49
bgp	680	2025年6月10日 00:00:00 - 00:30:00
backward	24	2025年6月10日 00:22:00 - 00:24:15
transition	20	2025年6月10日 00:19:38 - 00:24:15

ShowNetネットワーク情報カスタマイズ前(2)

検索

@FlowInspector mini

Generative AI Packet AnalyzeR (GAIPAR)

version 1.0.2

- TOPページ
  - 統合分析レポート
    - 1. 個別レポート情報
      - (1) 個別分析でユーザーが入力し...
      - (2) 個別分析で検索したkeyword内...
    - **2. 統合分析レポート**
      - (1) 個別レポートで出力された問...
      - (2) 個別レポートの問題点とされ...
      - (3) flow統計情報についての分析
      - (4) 詳細ログ内容の技術的な詳細...
      - (5) 詳細ログ内容が出力されるト...
      - (6) 追加調査が必要となる送信元IP...
      - (7) 問題点に対する具体的な対策
      - (8) 対策を実現するための具体的...
      - (9) 分析結果まとめ

Markdownをダウンロード

コンフィグファイルを編集

2. 統合分析レポート

(1) 個別レポートで出力された問題点

- OSPFプロトコルによるデフォルトルートの変更
- 隣接ルータの状態変化
- BGPのオープンメッセージエラー
- BGPのNLRI不一致
- BGPの状態遷移の不安定性

(2) 個別レポートの問題点とされた詳細ログ

- **IPV4 default Route is changed**: OSPFプロトコルによるデフォルトルートの変更が発生。
- **Neighbor changes event**: 隣接ルータの状態が「Loading」から「Full」に遷移。
- **Open Message Error**: BGPのオープンメッセージでサポートされていない機能が要求された。
- **NLRI Mismatch**: BGPのNLRIが不一致。
- **Backward Transition**: BGPの状態遷移が高い番号から低い番号に移行。

(3) flow統計情報についての分析

省略

ShowNetネットワーク情報カスタマイズ前(3)

検索

@FlowInspector mini

Generative AI Packet AnalyzeR (GAIPAR)

version 1.0.2

Markdownをダウンロード

コンフィグファイルを編集

(4) 詳細ログ内容の技術的な詳細解説

- OSPFのデフォルトルート変更は、ネットワークトポロジーの変化や隣接ルータの接続状態の変化によって発生します。
- BGPのオープンメッセージエラーは、サポートされていない機能が要求された場合に発生し、BGPセッションの確立に影響を与えます。
- BGPのNLRI不一致は、ルーティング情報の交換が正しく行われない原因となります。

(5) 詳細ログ内容が出力されるトラブルの具体例

- ネットワークのトポロジー変更によるルーティングの不安定化。
- BGPセッションの確立失敗によるルーティング情報の欠如。
- 隣接ルータの不安定な状態遷移によるネットワークの不安定性。

(6) 追加調査が必要となる送信元IPアドレス・送信先IPアドレス・MACアドレス・プロトコル・ポート番号

省略

(7) 問題点に対する具体的な対策

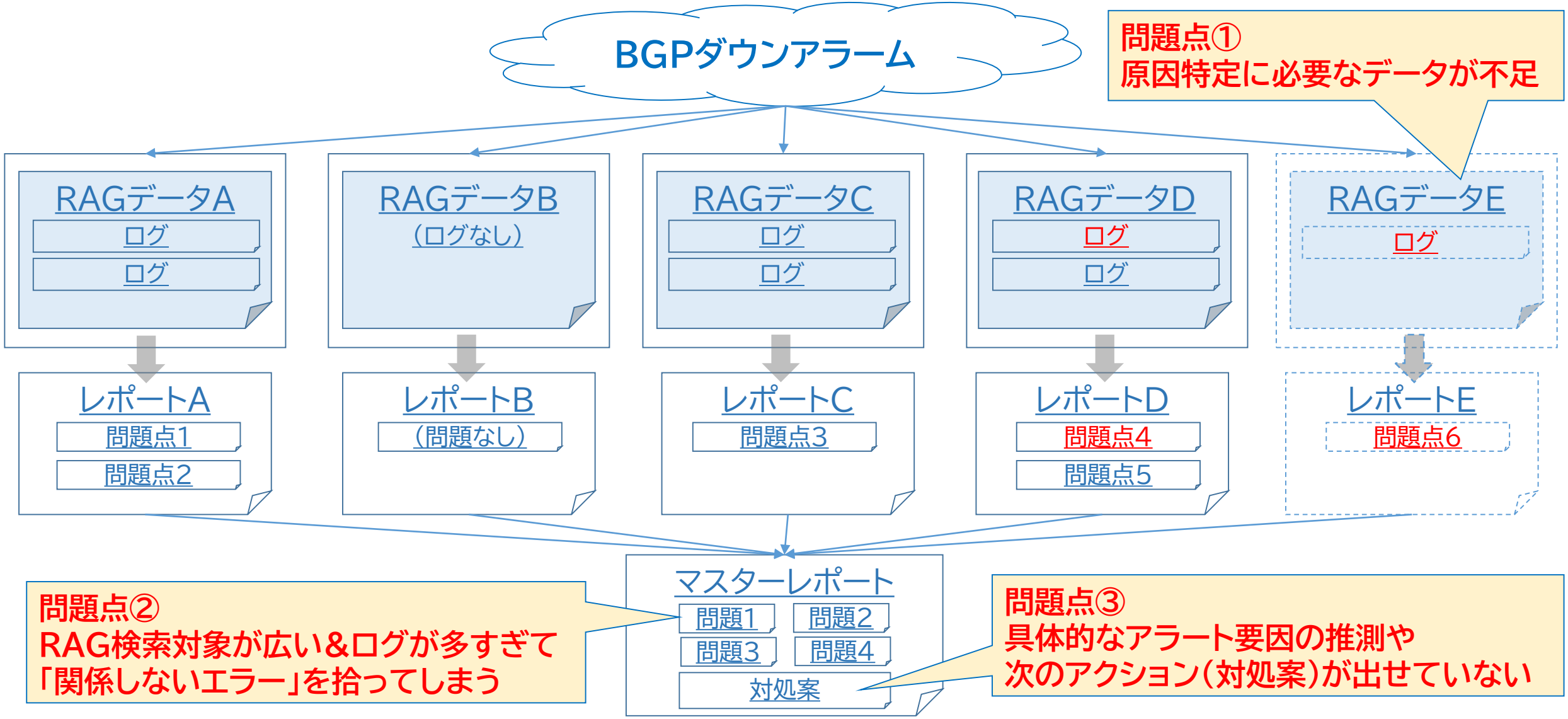
- OSPFの設定を見直し、隣接ルータの安定性を確認する。
- BGPの設定を確認し、サポートされている機能のみを使用する。
- BGPのNLRI設定を確認し、不一致がないように設定を修正する。

(9) 分析結果まとめ

このレポートでは、OSPFとBGPに関連する問題が特定されました。特に、BGPのオープンメッセージエラーやNLRI不一致がネットワークの安定性に影響を与えている可能性があります。これらの問題を解決するために、設定の見直しと適切な対策を講じることが重要です。

間違ったことは言っていないが…？

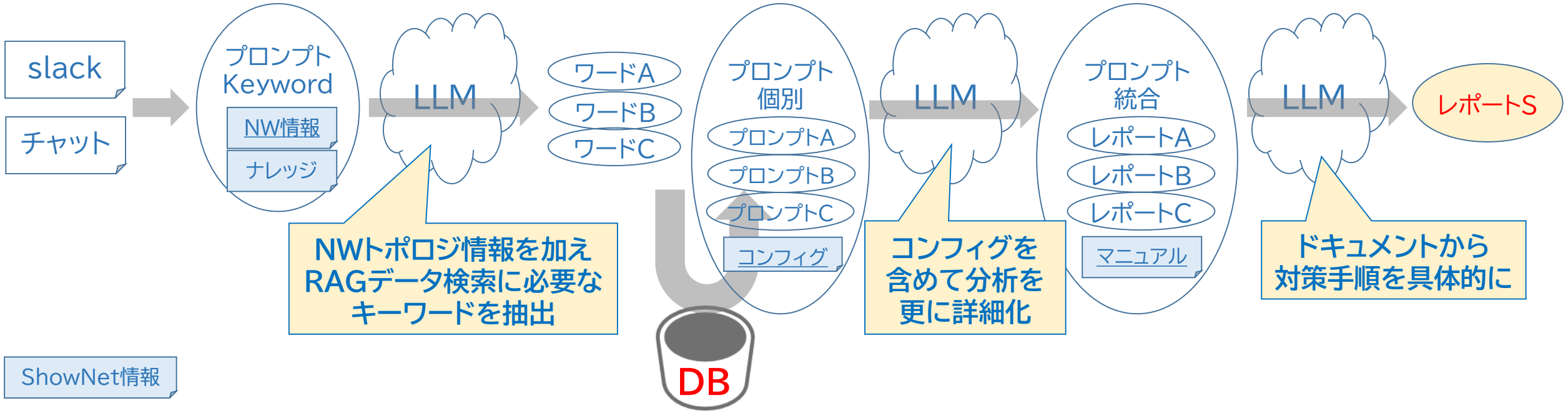
ネットワーク情報カスタマイズ前の問題点



“ShowNet ネットワーク情報”によるRAGカスタマイズ

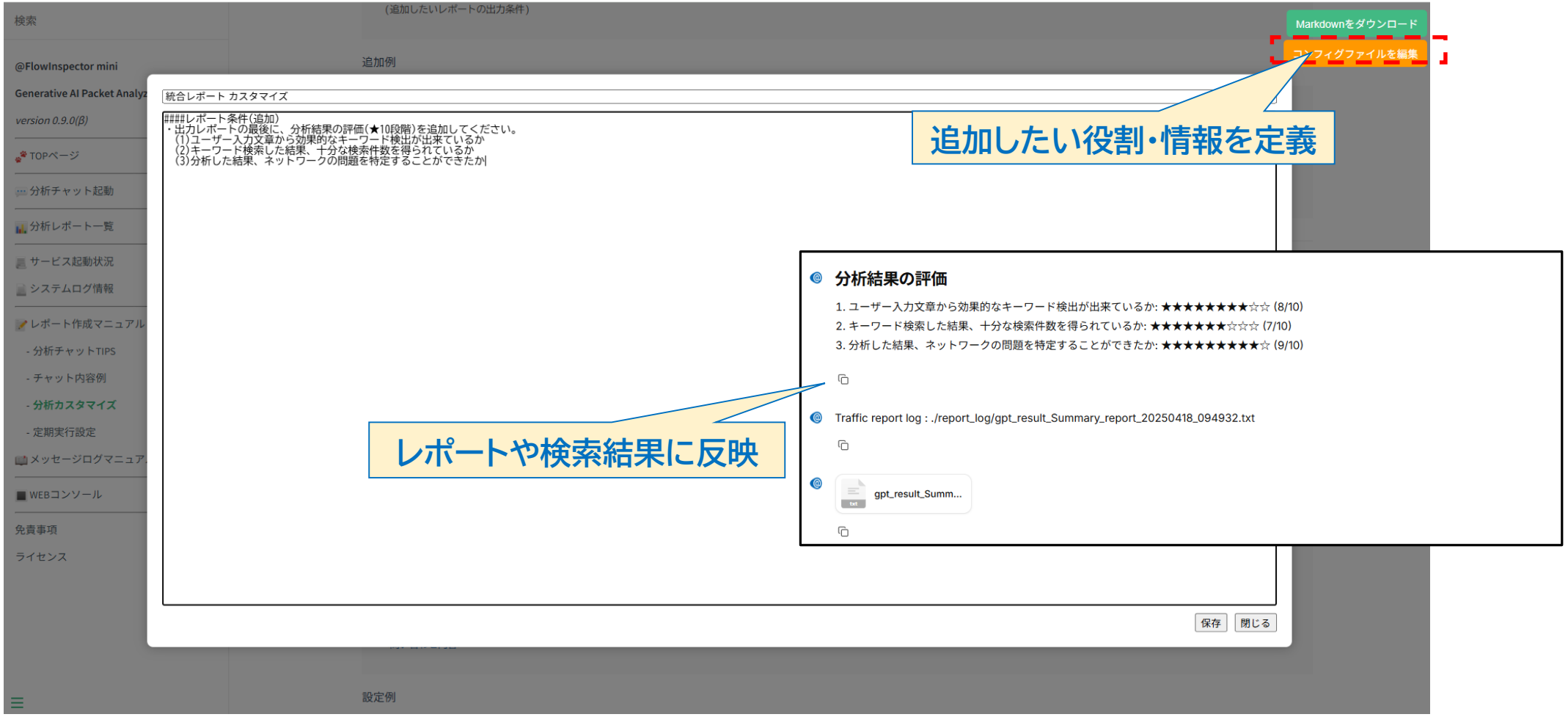
（1）「パケットログ検索に適したキーワード」の抽出精度向上
＋ NW構成管理表 ⇒ 「アラート」「チケット」関連機器情報（ホスト名、IPアドレスなど）の追加
＋ 障害分析ナレッジ ⇒ 「障害分析で検索するべきメッセージ・プロトコル情報」の追加

（2）「ネットワークトラブル分析レポート」の分析力強化
＋ ルータ・スイッチコンフィグ情報 ⇒ 「トラブル発生事象に関連する機器情報」の追加
＋ ネットワークポリシー・マニュアル情報 ⇒ 「解決するための対処案・アクション情報」の追加



解析レポートカスタマイズによるRAG強化機能

ネットワーク独自のカスタマイズを行うため、カスタムロール機能を使用
ShowNetのネットワーク情報を与えることで、トラブルシューティング力を強化する



ShowNet ネットワーク情報追加後の分析結果(1)

検索

@FlowInspector mini

Generative AI Packet AnalyzeR (GAIPAR)

version 1.0.2

- TOPページ
  - 統合分析レポート
    - 1. 個別レポート情報
      - (1) 個別分析でユーザーが入力し…
      - (2) 個別分析で検索したkeyword内…
    - 2. 統合分析レポート
      - (1) 個別レポートで出力された問…
      - (2) 個別レポートの問題点とされ…
      - (3) 詳細ログ内容とアラーム内容…
      - (4) アラームの発生原因と想定さ…
      - (5) 発生原因に対する切り分け方法
      - (6) 障害切り分けが必要なホスト…
      - (7) 分析結果まとめ
- 分析チャット起動

Markdownをダウンロード

コンフィグファイルを編集

1. 個別レポート情報

(1) 個別分析でユーザーが入力したプロンプト(アラーム)

- Problemin1m25s: SNMP Trap BGP Backward Transition Host ce5732h.pod8s[redacted] Event time 2025.06.10 00:27:49 Severity Average Opdata 20250610:002749 BGP Backward Transition [.1.3.6.1.2.1.15.7.2] "40" | 1 Event tags Application: SNMP Trap 設定済み: PARENT: nexus93400ld-h1.noc

(2) 個別分析で検索したkeyword内容、ヒット件数、時間(表形式)

Keyword	ヒット件数	時間範囲
[redacted]&ce5732h.pod8s	431	2025年6月9日 23:01:59 - 2025年6月10日 00:31:43
BGPBackwardTransition&ce5732h.pod8s	0	2025年6月10日 00:27:49
Backward&ce5732h.pod8s	4	2025年6月9日 23:47:02 - 2025年6月10日 00:29:10
Transition&ce5732h.pod8s	0	2025年6月10日 00:27:49
isis&ce5732h.pod8s	0	2025年6月10日 00:27:49
ospf&ce5732h.pod8s	82	2025年6月9日 23:07:51 - 2025年6月10日 00:27:49
bgp&ce5732h.pod8s	31	2025年6月9日 23:46:53 - 2025年6月10日 00:29:42
vni&ce5732h.pod8s	0	2025年6月10日 00:27:49
vxlan&ce5732h.pod8s	0	2025年6月10日 00:27:49
linkdown&ce5732h.pod8s	8	2025年6月9日 23:07:51 - 2025年6月9日 23:46:53
linkup&ce5732h.pod8s	8	2025年6月9日 23:07:18 - 2025年6月10日 00:26:17

他の利用プロトコル(OSPF)・Linkdown/up情報を調査

分析対象機器のログに情報を限定

ShowNet ネットワーク情報追加後の分析結果(2)

検索

@FlowInspector mini

Generative AI Packet AnalyzeR (GAIPAR)

version 1.0.2

Markdownをダウンロード

コンフィグファイルを編集

2. 統合分析レポート

(1) 個別レポートで出力された問題点

- BGPの状態遷移に関する問題が複数のログで確認され、特にBGP FSMが高い番号の状態から低い番号の状態に移行している。
- OSPFの隣接ルータがダウン状態に遷移している。
- 複数のインターフェースがDOWN状態に遷移している。

分析アラームに関連する問題点のみ抽出

(2) 個別レポートの問題点とされた詳細ログ

- `LOCAL1.CRIT: Jun 10 2025 00:29:10.223.1+09:00 ce5732h.pod8s BGP/2/BACKWARD:OID 1.3.6.1.2.1.15.7.2 The BGP FSM moves from a higher numbered state to a lower numbered state. (BgpPeerRemoteAddr=[redacted], InstanceId=0, Afi=25, Safi=70, PeerType=1, PeerRemoteAddr=[redacted], InterfaceIndex=0, BgpPeerLastError=40, BgpPeerState=1, BgpPeerUnavaiReason=4, InterfaceName=null)`
- `LOCAL1.CRIT: Jun 9 2025 23:07:51.111113 ce5732h.pod8s %%01OSPF/3/NBR_CHG_DOWN(l)[7787]:Neighbor event:neighbor state changed to Down. (ProcessId=290, NeighborAddress=[redacted], NeighborEvent=KillNbr, NeighborPreviousState=Full, NeighborCurrentState=Down)`
- `LOCAL1.ALERT: Jun 9 2025 23:07:50.973.1+09:00 ce5732h.pod8s IFNET/1/IF_LINKDOWN:OID 1.3.6.1.6.3.1.1.5.3 Interface 55 turned into DOWN state.(AdminStatus=1,OperStatus=2,InterfaceName=25GE0/0/1)`

(3) 詳細ログ内容とアラーム内容の因果関係

- BGPの状態遷移ログは、BGPピアとの接続が失われたことを示しており、これはインターフェースのDOWN状態がトリガーとなっている可能性が高い。
- OSPFの隣接ルータがダウンしたログは、物理インターフェースの状態変化が原因であることが示唆されている。
- インターフェースのDOWN状態のログは、物理的な接続不良や設定ミスが原因である可能性がある。

ShowNet ネットワーク情報追加後の分析結果(3)

検索

@FlowInspector mini

Generative AI Packet AnalyzeR (GAIPAR)

version 1.0.2

Markdownをダウンロード

コンフィグファイルを編集

(4) アラームの発生原因と想定される事象

- **物理障害の観点**: インターフェースの物理的な接続不良やケーブルの断線が原因で、リンクダウンが発生し、BGPおよびOSPFの状態遷移に影響を与えている可能性がある。
- **論理障害の観点**: BGPおよびOSPFの設定ミスや、タイムアウト設定の不適切さが原因で、プロトコルの状態遷移が不安定になっている可能性がある。

(5) 発生原因に対する切り分け方法

機器に対応した「次のアクション」を提示

- **物理切り分け**:
  - インターフェースの物理接続を確認し、ケーブルやポートの状態をチェックする。
  - `show interface` コマンドを使用して、インターフェースの状態を確認し、エラーや不具合がないかをチェックする。
- **論理切り分け**:
  - BGPおよびOSPFの設定を確認し、タイムアウト設定やリトライ設定が適切であるかを確認する。
  - `show ip bgp` および `show ip ospf neighbor` コマンドを使用して、プロトコルの状態を確認し、問題が発生しているピアや隣接ルータの設定を見直す。

(6) 障害切り分けが必要なホスト名・IPアドレス(表形式)

省略

(7) 分析結果まとめ

- BGPの状態遷移とOSPFの隣接ルータの状態変化は、インターフェースのリンクダウンに起因している可能性が高い。物理的な接続不良や設定ミスが原因である可能性があるため、インターフェースの物理接続とプロトコルの設定を重点的に確認する必要がある。
- 物理的な接続不良が疑われる場合は、ケーブルやポートの交換を検討し、設定ミスが疑われる場合は、BGPおよびOSPFの設定を見直すことが推奨される。

「BGPダウンの原因は物理IFダウン」と推測出来ている

カスタマイズによって得られた精度向上の効果(推測)

① PODからBGP downアラート発報を確認

② PODのログ・設定を確認
(1)BGP downの原因が”Hold Timer Expired”であること
(2)BGP対向がxx.xx.xx.xxであること
(3)直前にospf neighbor statusが一度downしてestablishしていること
(4)さらに直前にinterface 25GE0/0/1が一度downしてUpしていること
} By Log
(5)interface 25GE0/0/1がアップリンク設定・状態であること
} By Config

③ 上記情報から時系列で原因を推測
物理down→ospf down→BGP hold time expired
の順に発生し、物理downがトリガーであることを把握

④ 物理linkを被疑箇所として、モジュール・ケーブル・中継区間の切り分けにうつる
} By Guide

アラート発報要因 ： アップリンクの物理レイヤトラブル

ShowNetトラブルシューティング効率化 まとめ

本システムは会期中も絶賛運用
しかし、「ShowNetのトラブルシューティング」は一筋縄ではいかない

① ログ情報量が膨大すぎる
- リアルタイムRAGデータの高速生成・高速検索の工夫が必要
- 「本当に有用なログ」を的確に見つけ出さないといけない

② 文章化されていない暗黙知情報の多さ
- 設営中と会期中のログは量も性質も対処も異なる
- 「砂漠の砂金」を探せる超技術者集団だから可能な芸当も多い
- ShowNetのNWトラブルに対する正解とは？

よりディープな内容はshownet.conf_2025で！

大規模NWチャレンジから得られた知見
ディスカッションしたい事項

LLM活用オペレーションへの知見

大規模NW実証から得られた知見

- 現在のLLMは「パケットログから有用なトラブル解析が出来る水準」に達している

- パケットやSyslogの適切なContext化は、解析精度を高める最も重要な要素
  - 「不要な情報を与えず、必要な情報を与える」という基本
  - 一般的なプロンプトエンジニアリング手法も(現時点では)重要

- 情報量が膨大になる大規模NWでは、LLM分析を多層化するメリットが大きい
  - 細かい情報はSLM、統合的な判断はLLMと使い分けるとコストも下がる
  - レイテンシを減らし、分析可能なトークン数をスケールさせることができる

- プロンプトの拡張性は絶対に残そう(全知全能プロンプト」は難しい)

まとめ・皆様とディスカッションしたい事項

「LLMを活用したNWオペレーション」は様々な要素が絡み合う複雑系
皆様から知見を頂き、精度とコストの最適解を探っていきたい

① 求める回答精度・品質(ゴール)
　サジェストまで ⇔ アクションが必要(ハルシネーション非許容)

② LLM問い合わせ頻度
　Q&A実行 ⇔ イベントドリブンで常に実行
　データ更新が不要　⇔　データのリアルタイム反映が必要

③ 必要なセキュリティ
　“非学習”で十分　⇔　外部通信不可