「生成AIを用いたネットワーク監視」の実運用課題と利用コスト
～そのLLM、いくらかかってますか？～

2026年7月15日

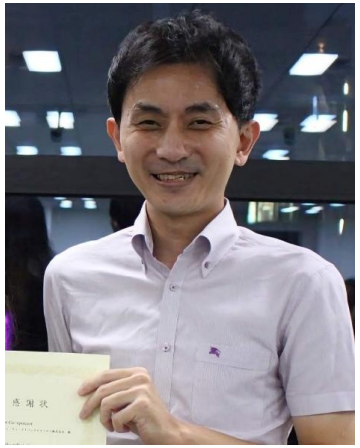
NTTアドバンステクノロジ株式会社

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)

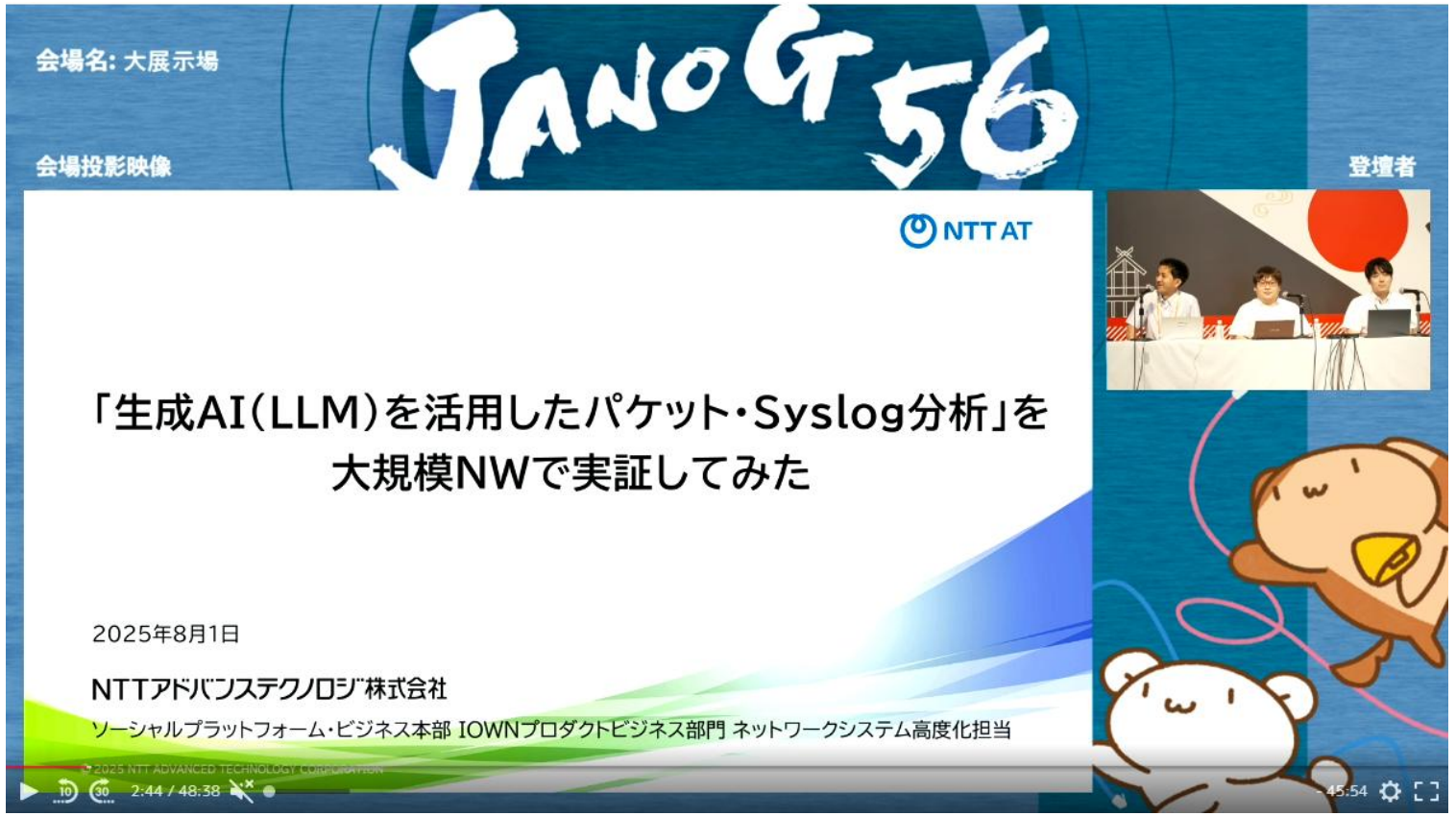
2011年入社。NGN開発・維持管理を複数担当した後、
NW新技術・製品開発チームに移動。
NWアクセラレータとしてのFPGA開発・アーキテクチャ検討の傍ら、
NTT-AT社のコントリビュータリーダを務めています。
最近は可処分所得の多くをトークンに費やしています。



レヌグンタ タンマイ

南インド出身。JANOGへの参加は今回で3回目です。
光NWや光データセンター分野での経験を経て、2022年に入社。
以来、製品開発チームにて、ネットワーク監視・分析に従事しています。
趣味はドラマ・映画鑑賞と写真撮影です。

JANOG 56(2025/8)プログラム



発表資料URL

「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
https://www.janog.gr.jp/meeting/janog56/ai-nwlogs/

JANOG 56の内容は雑誌でも取り上げて頂きました

日経NETWORK

2026年5月号

この号の目次へ »

特集1
AIとネットワーク運用
先行10社が明かす勘所

特集2
認証の転換点
パスキーで不正ログイン対策はどう変わるか

特別リポート
数千の脆弱性見つける「Claude Mythos」の衝撃
セキュリティーの常識が覆るか

ネスペ試験で学ぶ ネットワーク技術のキホン
送信ドメイン認証

購読のお申し込み　PDFダウンロード（有料会員）

お知らせ

AI・量子・E2E・光電融合・遠隔施工、注目技術の展示会「日経クロステックNEXT」開催！

世界が注目する「大気水生成」、海外スタートアップ登壇【5/29開催】

【特別セミナー】地政学リスク時代の不動産戦略　6/4開催（オンライン・無料）

有料会員の皆様へ 大切なお知らせ（ご継続時の期間・料金のご案内方法変更）

編集部からのお知らせ

雑誌記事HTMLを読むには

雑誌読者の登録方法

雑誌最新号
Latest Issue

日経コンストラクション　2026年5月号
始動、新インフラ強靭化

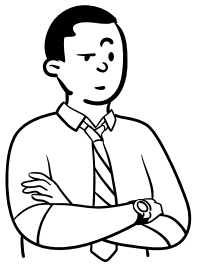
「日経クロステック – 日経NETWORK 6月号」より引用
https://speakerdeck.com/shownet/zhan-shi-hui-chang-nei-shuo-ming-suraido-monitaringu-shownet-2025

サービス運用例1　：ネットワークの健康診断レポート

お困りごと

① インターネットに抜ける通信量が多いときにNW全体が遅くなるが、どのロケーションからの流量が多かったのかを簡易に把握することができない。

② 重要データがインターネットに流出していないかを確認したい。



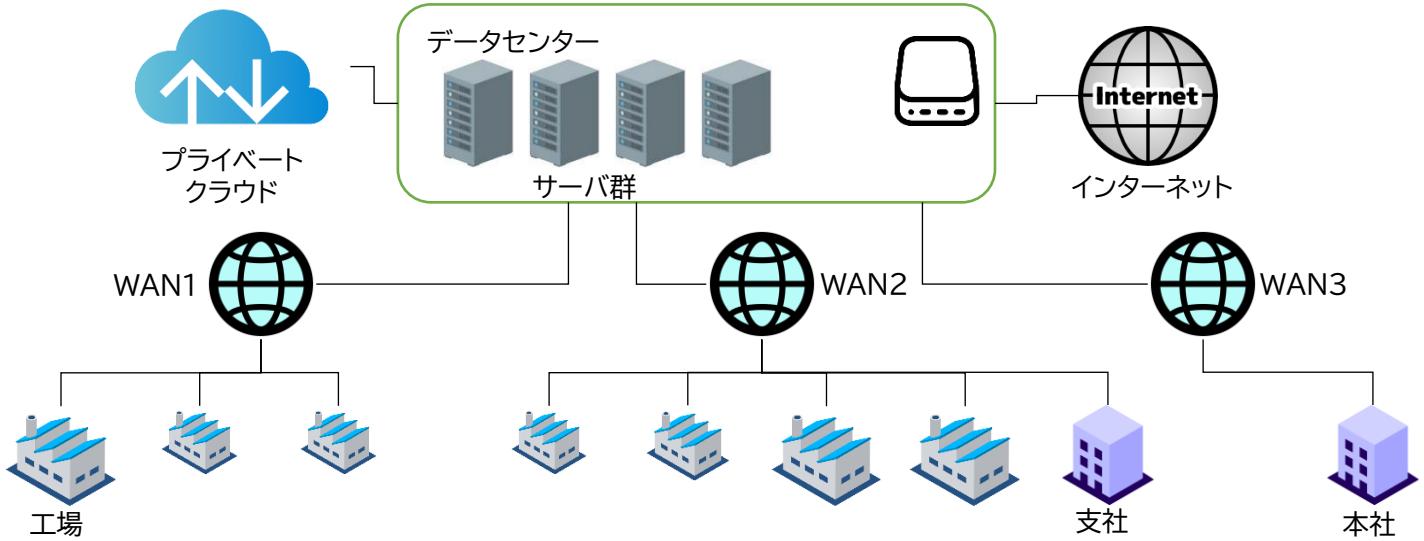
【導入後】

インターネットへの出口回線(1Gbps)にを設置して、外向けのトラフィックをミラーリングで取り込むことで、どのロケーションからの流量が多かったのかを簡易に把握できるようになった。
サーバー群のIPアドレスから外への通信に、普段と変化がないかを解析依頼することで、状況を簡易に把握できるようになった。解析を定期実施させて、毎日のレポートを比較する運用を実施している。

【Before】:インターネットへの通信量が増え、NW全体が遅くなっても、どの拠点からの流量が多いのか簡単に把握できない。重要データが外部に流出していないかを確認する手段がない。

⇒

【After】:どの拠点からの通信量が多いかを簡易に把握できるようになった。サーバー群(重要データが保管されているサーバーを含む)の外向け通信を解析し、普段と異なる挙動を把握可能になり、さらに定期解析とレポート比較を運用に組み込み、流出リスクを早期に把握できるようになった。



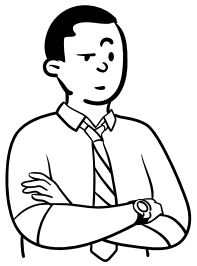
サービス運用例2：NWトラブルシューティングの効率化

NTT AT

お困りごと

① ネットワークが「つながらない」「遅い」という申告があった際に、どんな通信が流れているか、何が原因なにかの解析は能力の高い熟練オペレーターにしかできず、解析に時間がかかる。

② 障害が発生する前段階で、不要な通信が一定量発生しているようだが、その段階では兆候として把握することができない。



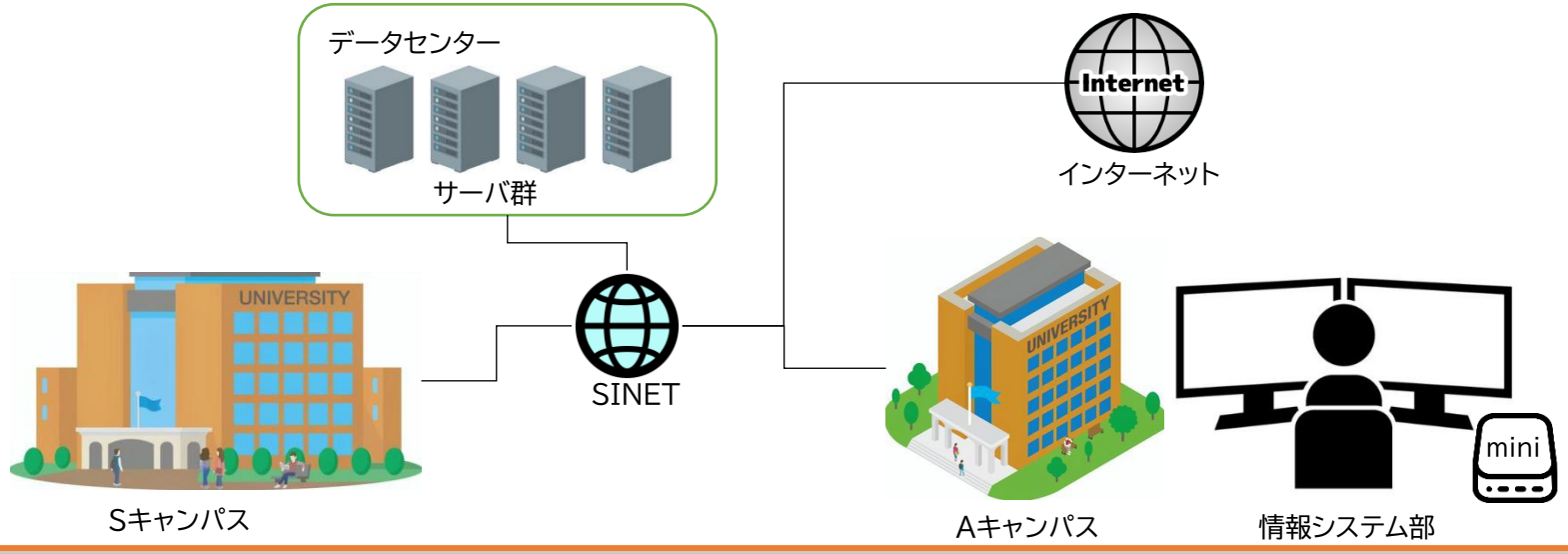
【導入後】

今まで能力の高いオペレーターがWireShark等で解析していた環境に導入することで、障害時に熟練オペレータに頼らずとも、どんな通信が流れているかを迅速に把握することができるようになり、原因解析のスピードが上がった。
また、障害発生前の段階で不要な通信を可視化し、障害の兆候を事前把握できるようになった。

【Before】
ネットワークが「つながらない」「遅い」と申告されたとき、原因解析は熟練オペレーターにしかできず、時間がかかる。障害発生前に不要な通信が増えていても、その兆候を把握できない。

⇒

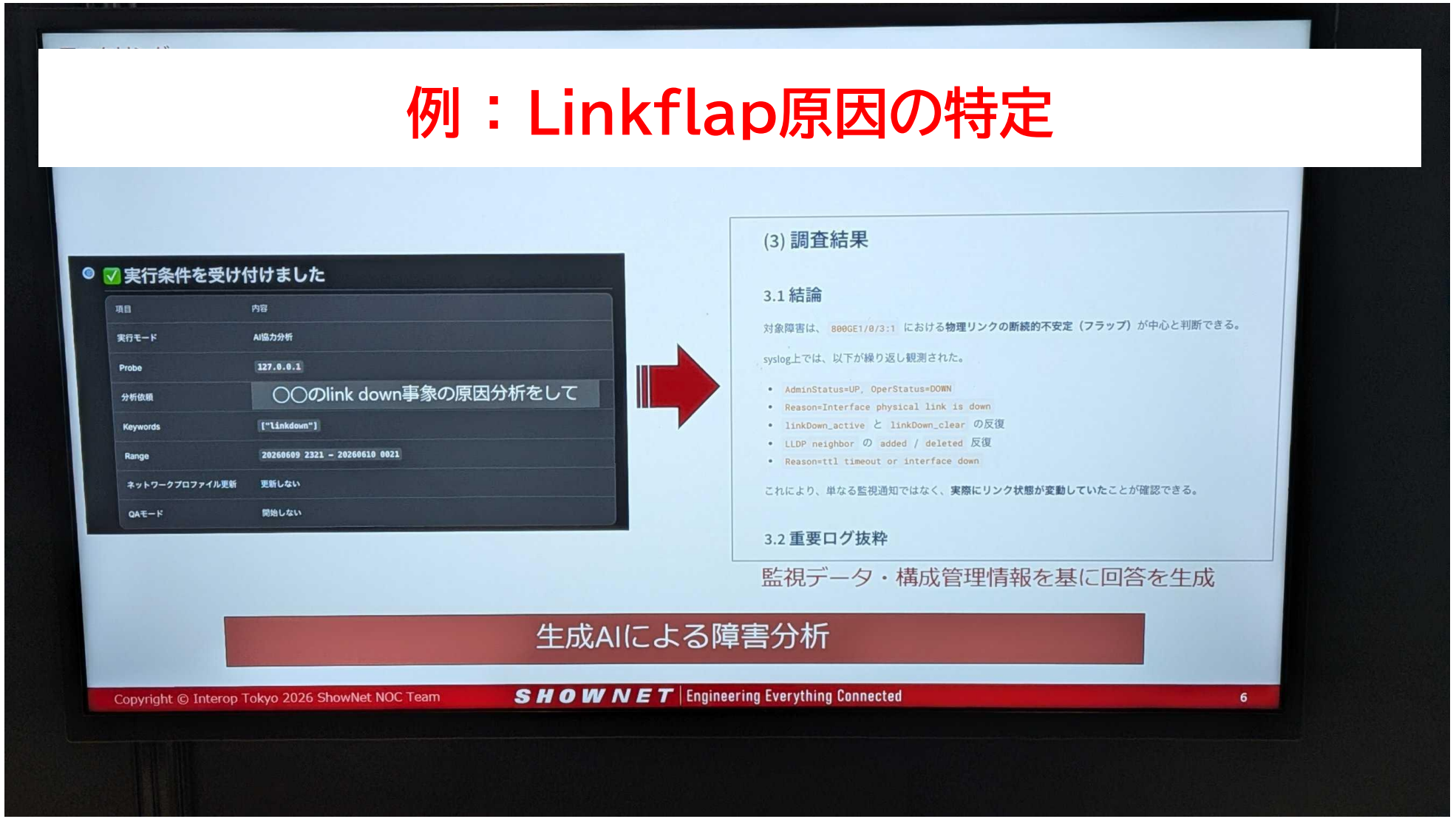
【After】
ネットワーク障害時に、誰でも簡単に通信状況を確認し、原因を迅速に推測できるようになった。
障害の兆候を事前に検知し、予防的な対応が可能になった。



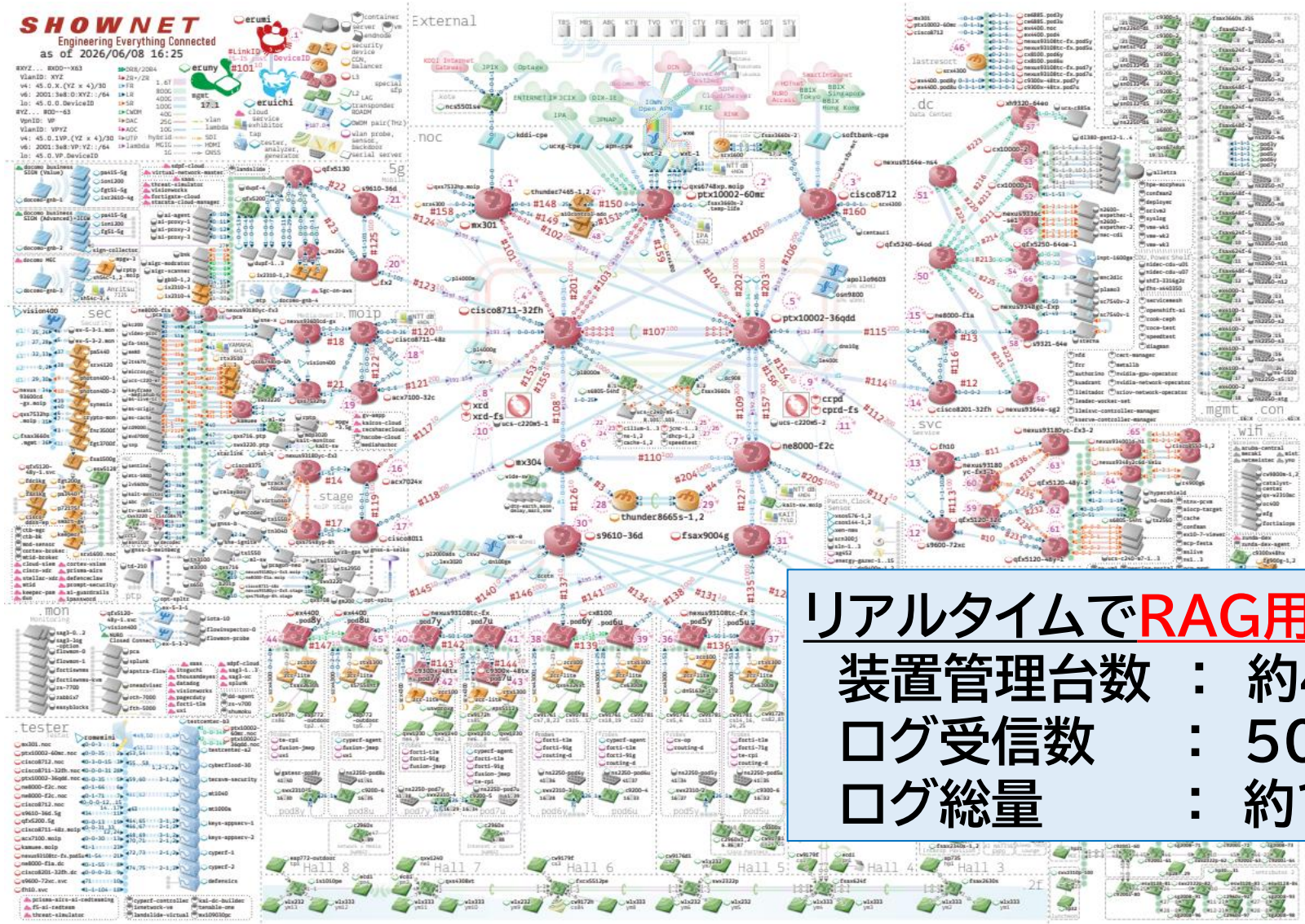
(補足)情報システム部の手元にキャンパス内の各VLANを流れるトラフィックをミラーリングできるようにしています。

Interop Tokyo 2026 ShowNet 実証実験(1)

Interop Tokyo 2026 ShowNet 実証実験(2)



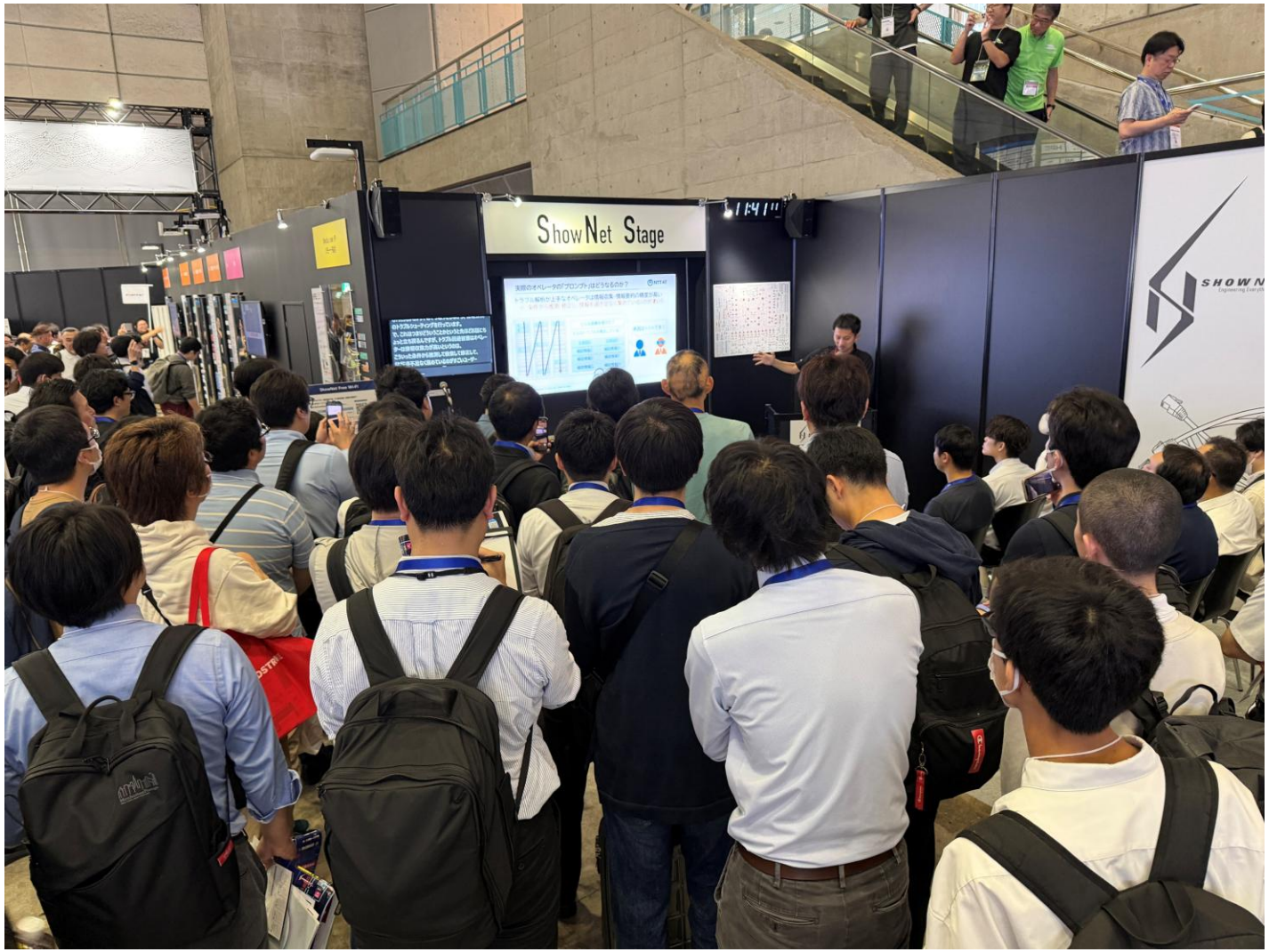
Interop Tokyo 2026 ShowNet ネットワーク図



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　　：　5000～10000[msg/sec]
ログ総量　　：　約1.5TB超(会期3日目)

Interop Tokyo 2026 ShowNet ステージ

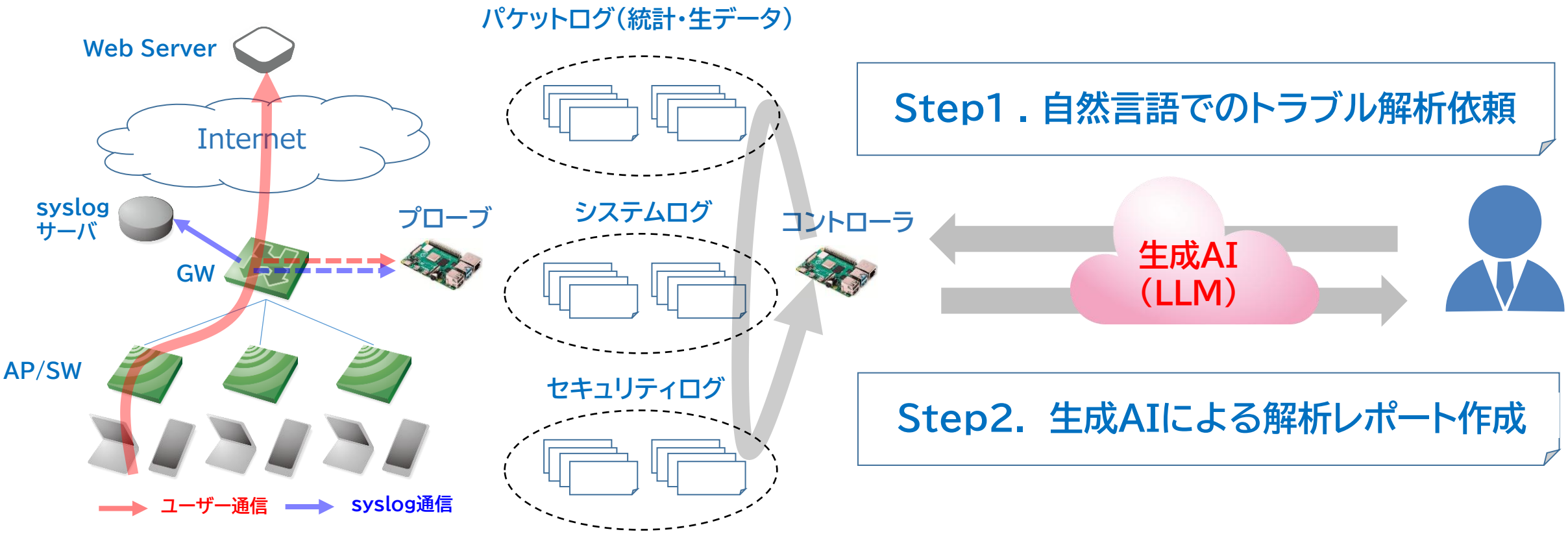


生成AIを用いたネットワーク・ログ監視サービス

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



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？

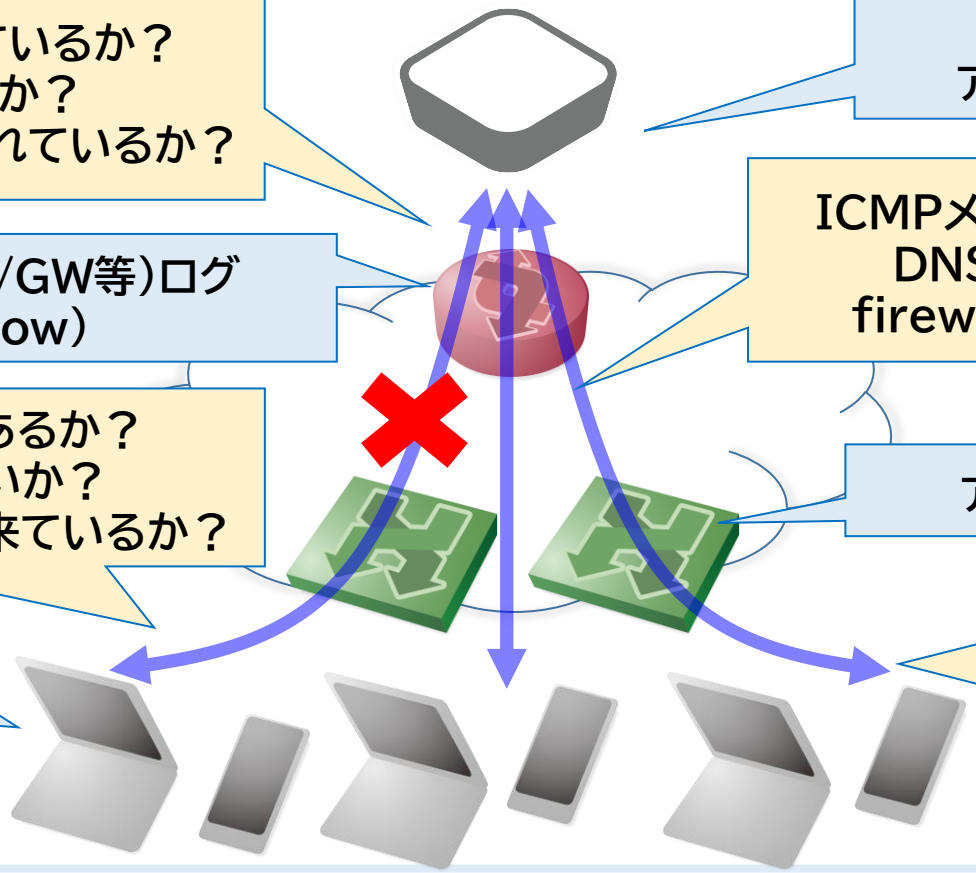
OS/OSSのログ
アプリケーションログ

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

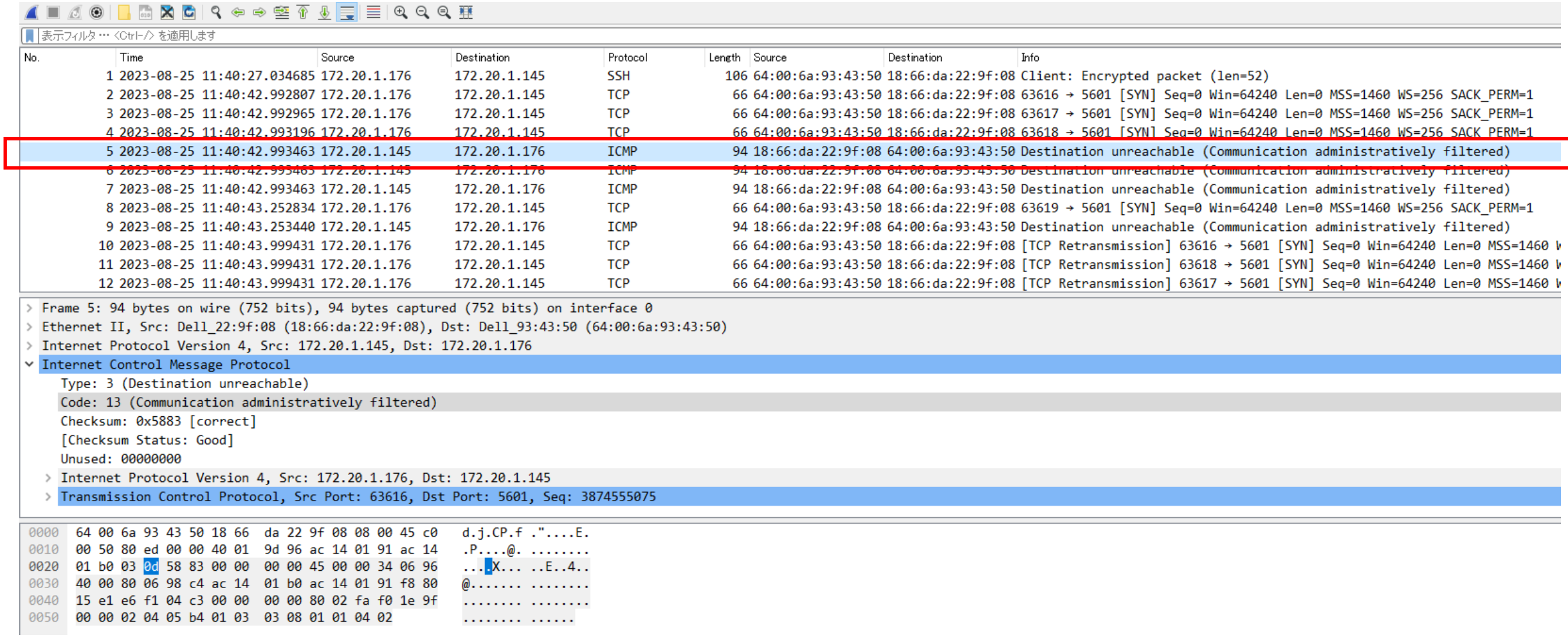


クライアント端末ログ
問題時の画面キャプチャ

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

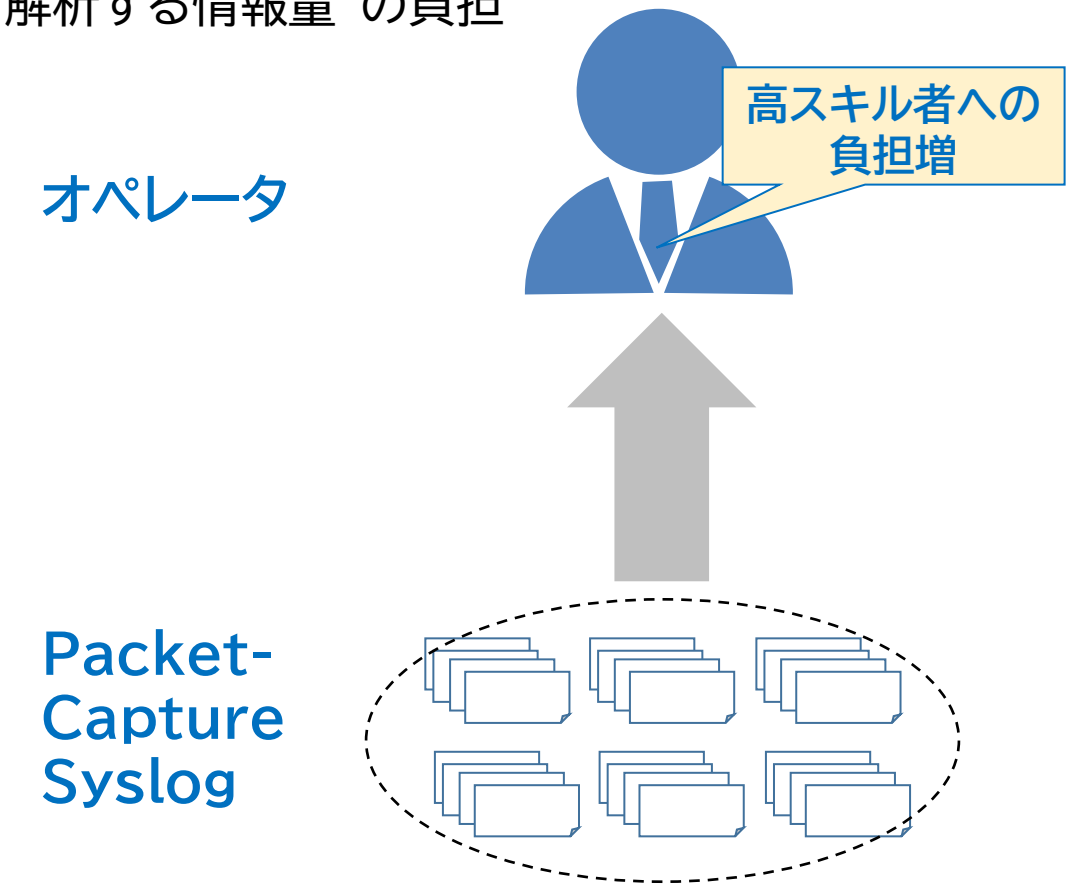
例 ： アプリケーション搭載Linuxサーバのfirewall設定漏れ



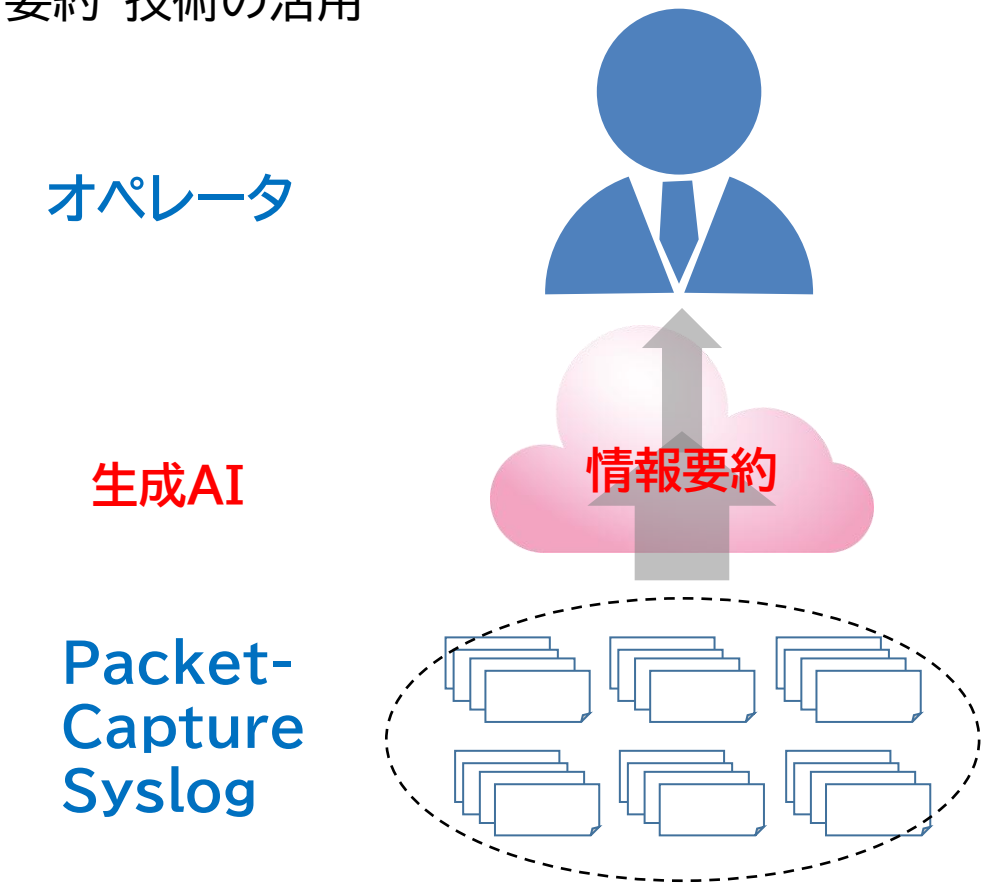
ネットワークオペレーションの課題と解決

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



どのようにサービス提供した(している)か？

提供形態

- 分析機器(ミニPCやサーバ)の貸し出し
- 年間サブスクリプション　＋ 機器手数料

利用方法

- チャット形式での分析実行
- 定期実行形式での分析実行

※ともに、LLMの回答結果内容のサポートはしない

本日お話しする内容（結論）

結局、生成AIによるネットワーク監視は出来るの？

⇒　LLMモデルの進化は想像以上
「十分に出来る」と言っていい水準
（他セッションの皆様の発表もぜひ！）

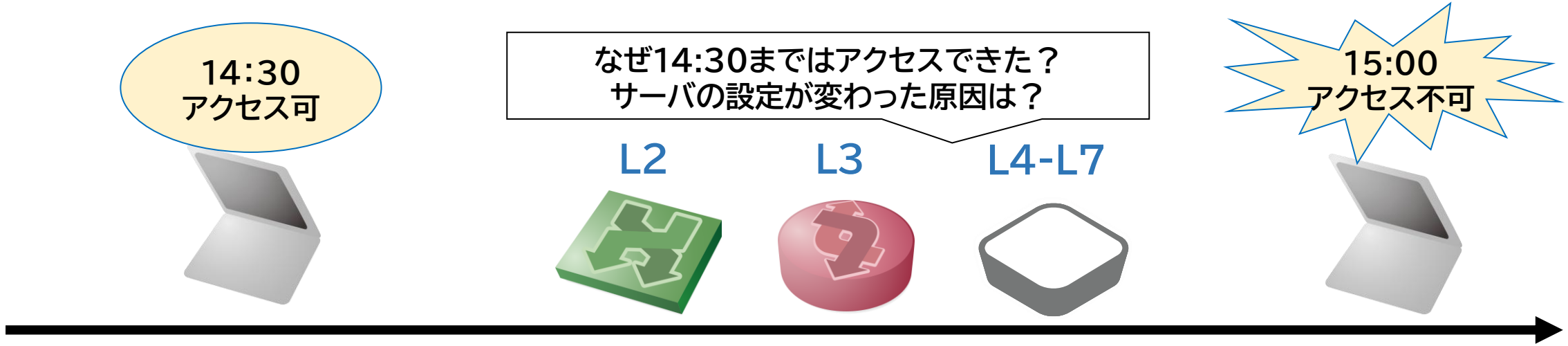
じゃあ何が今の課題なの？

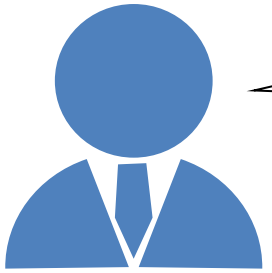
⇒　使うための“コスト”がかかる💢💢💢

生成AIによるネットワーク監視とコスト
～大規模ネットワーク実証の課題を例として～

「トラブルシューティング」の質・精度を決めるものとは

NWオペレーションにおけるトラブルシューティングでは、
解析情報の的確な把握と、それに基づく行動が非常に重要
　≒ “NWオペレータの熟練度は、情報収集の精度と相関がある”





・14時半から15時の間にサービスアクセス不可となった【ユーザー申告情報】
・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 【ログ情報】
・FWのコンフィグ設定が誤っている 【ログ情報】
　⇒ アクセス不可の原因はFWの設定漏れだが、なぜいきなり？
・FWサービスを再起動する工程があった 【スケジュール情報・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）

究極の解析依頼プロンプト

「トラブルの元となっている全ての情報のみ」を与えているプロンプト

＃解析依頼プロンプト

プロンプトの意味

トラブル内容

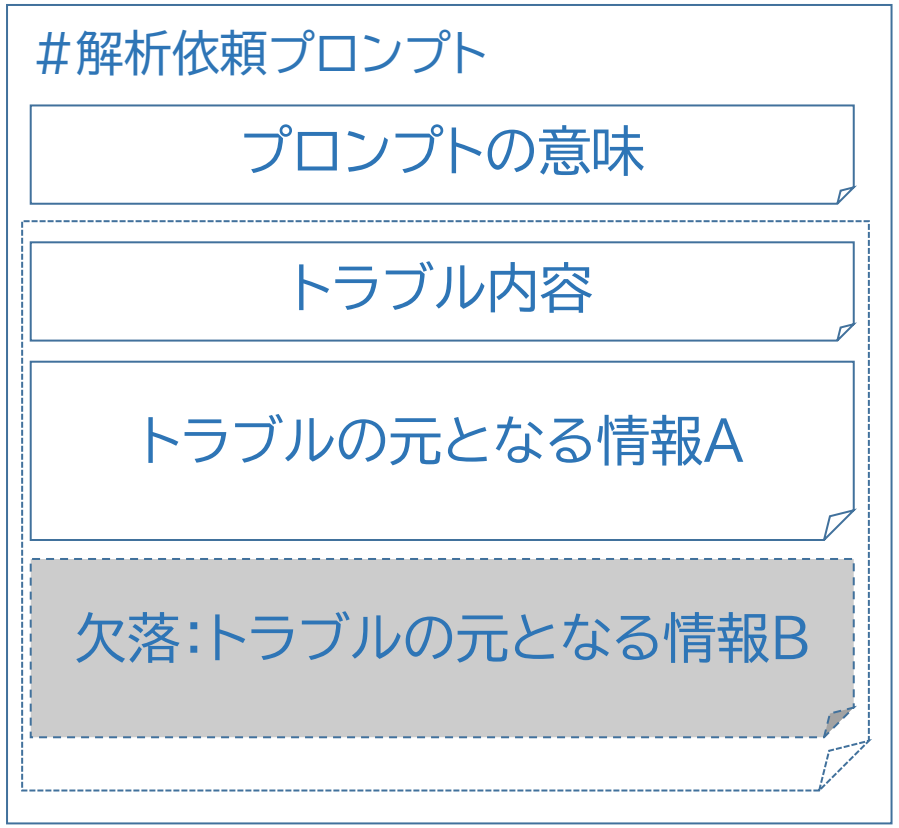
トラブルの元となる情報

トラブル原因は●●です！
例：コンフィグ誤り

トラブル解析プロンプトの現実的な問題 – 情報欠落

「トラブルの元となっている全ての情報のみ」を与えているプロンプト

⇒　プロンプトにトラブル原因を含められないと、解析できない



原因を特定できません！

トラブル解析プロンプトの現実的な問題 – 情報過多

「トラブルの元となっている全ての情報のみ」を与えているプロンプト

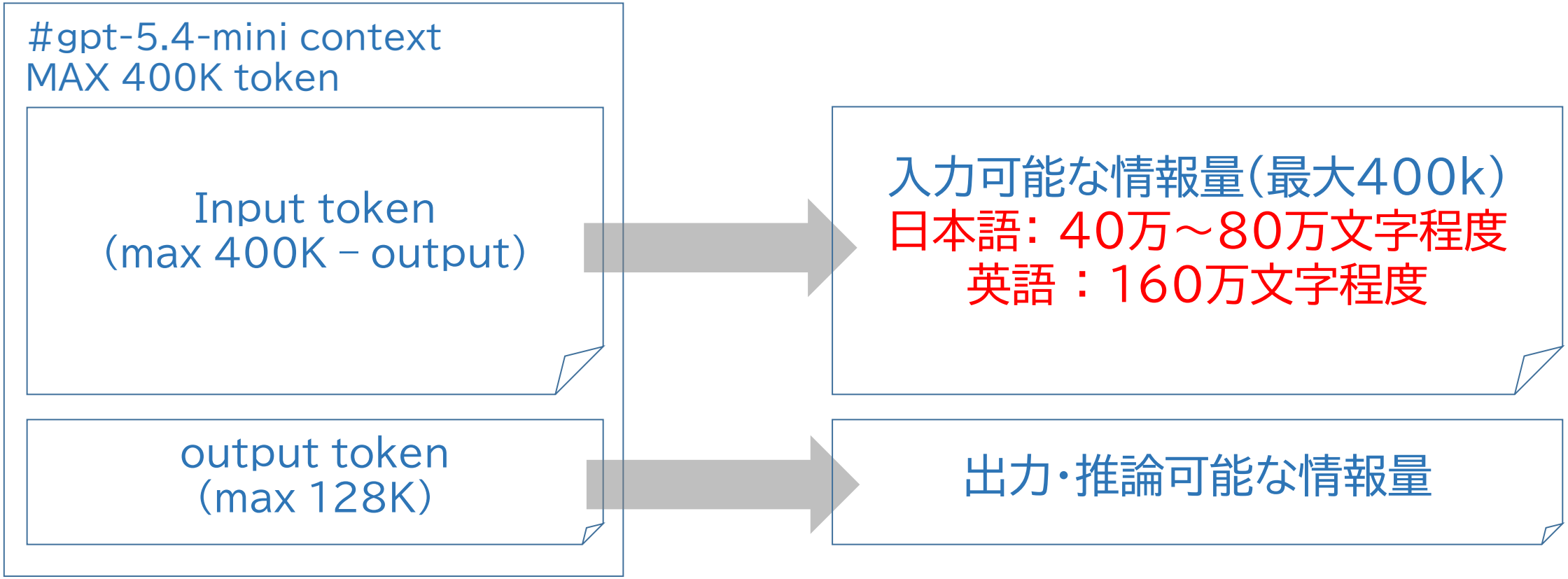
⇒　情報に不要な情報が多すぎると、ハルシネーションが起こる？

トラブル原因は××です！（嘘）

ノイズが多い＝ハルシネーションが起こる
これは問題の本質ではない

おさらい：LLM解析プロンプトにおける「情報量」(1)

入力可能なトークンはモデルで変化するが、最新モデルで400K～1M程
⇒ 概ね1トークンで1文字(日)～4文字(英)を表現することが出来る



gpt-5.4：入出力合わせて1Mまで
gpt-5.4-mini：入出力合わせて400Kまで

おさらい：LLM解析プロンプトにおける「情報量」(2)

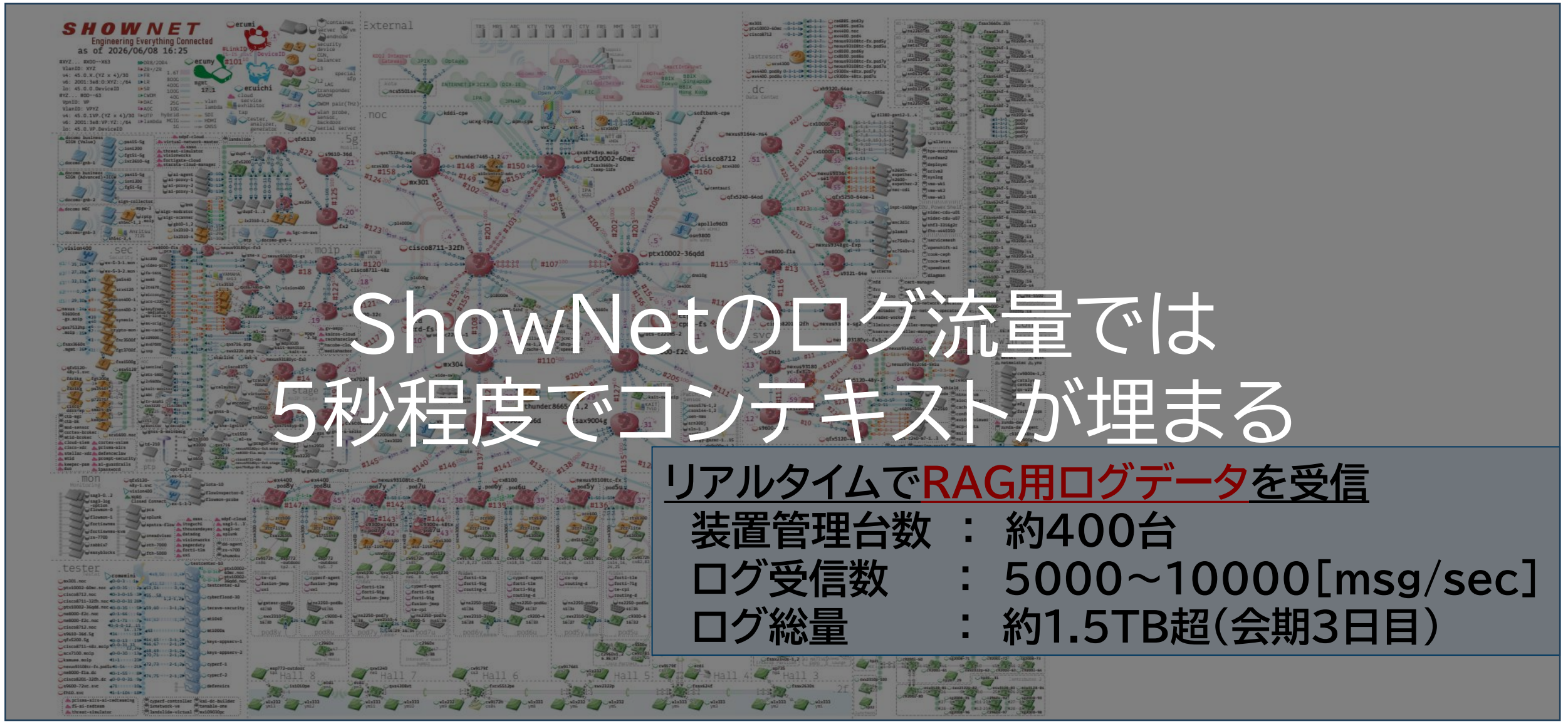
一回のプロンプトに入るログは最大でも40000件程度

●BGP Peer Downのログ≒108文字≒25～40トークン程度消費する
Jun 8 10:15:23 router01 %BGP-5-ADJCHANGE: neighbor 192.0.2.10 Down BGP Notification sent; hold time expired

コンテキスト上限	ログ件数(1ログ約100文字前後と概算)
272K tokens	6000件～10000件
400K tokens	10000件～15000件
1M tokens	25000件～40000件

※システムプロンプトや出力トークンもあるため、可能な件数は上表より減る

例：大規模ネットワーク（ShowNet）のログ流量



ShowNetのログ流量では
5秒程度でコンテキストが埋まる

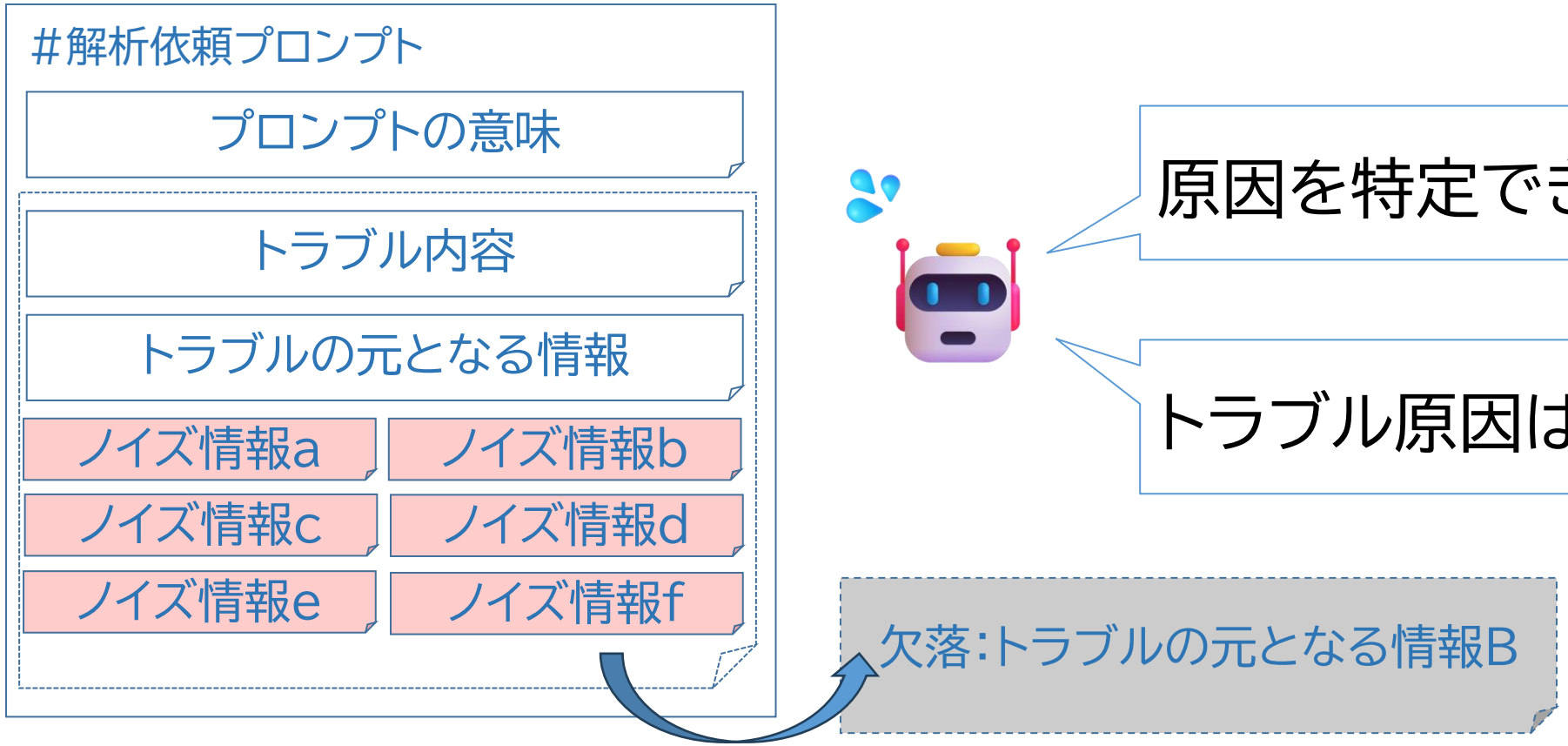
リアルタイムでRAG用ログデータを受信

装置管理台数　：　約400台
ログ受信数　　：　5000～10000[msg/sec]
ログ総量　　：　約1.5TB超（会期3日目）

大規模NWにおけるトラブル解析プロンプトの困難さ

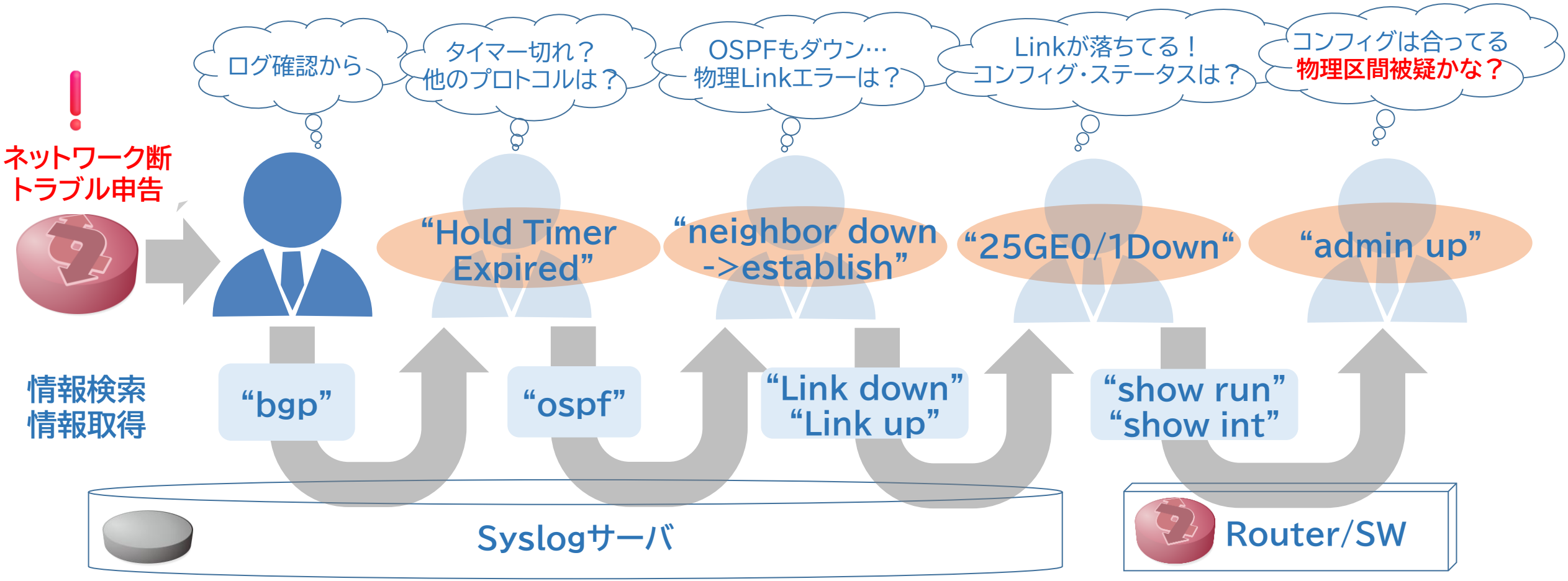
「トラブルの元となっている全ての情報のみ」を実現できないのは？

⇒ 「情報の過多」による「情報の欠落」が最も根本的な問題



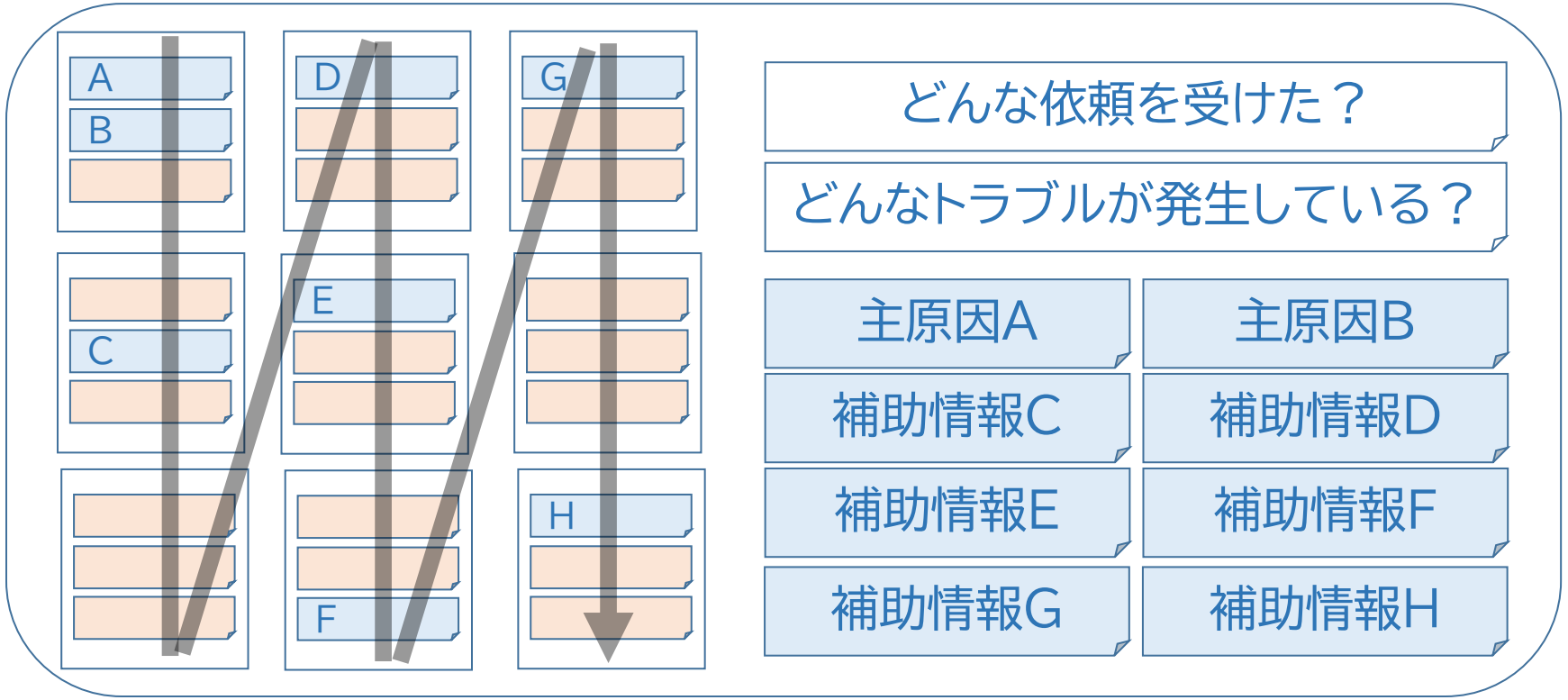
トラブルシューティング実例(BGP Downアラート)

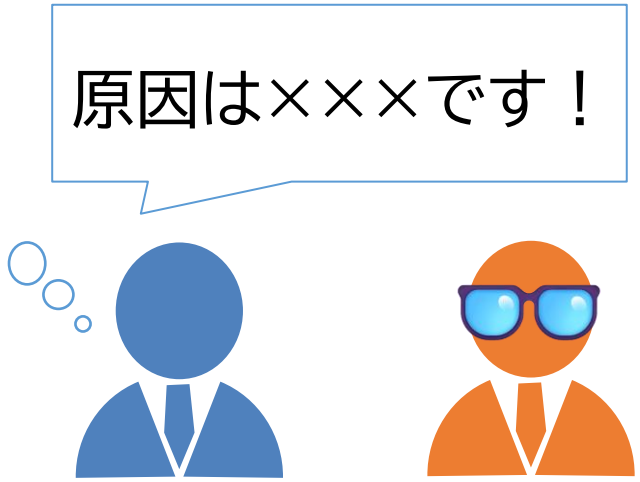
NWオペレータは、様々な装置から情報を取捨選択して、トラブルを切り分けていく
⇒ 実際のオペレータは「大きくまとめて」ではなく「小さく細かく」解析している



実際のオペレータの「プロンプト」はどうなるのか？

トラブル解析が上手なオペレータは情報収集・情報要約の精度が高い
⇒　条件から推測・修正し、情報を過不足なく集めている（のが凄い）

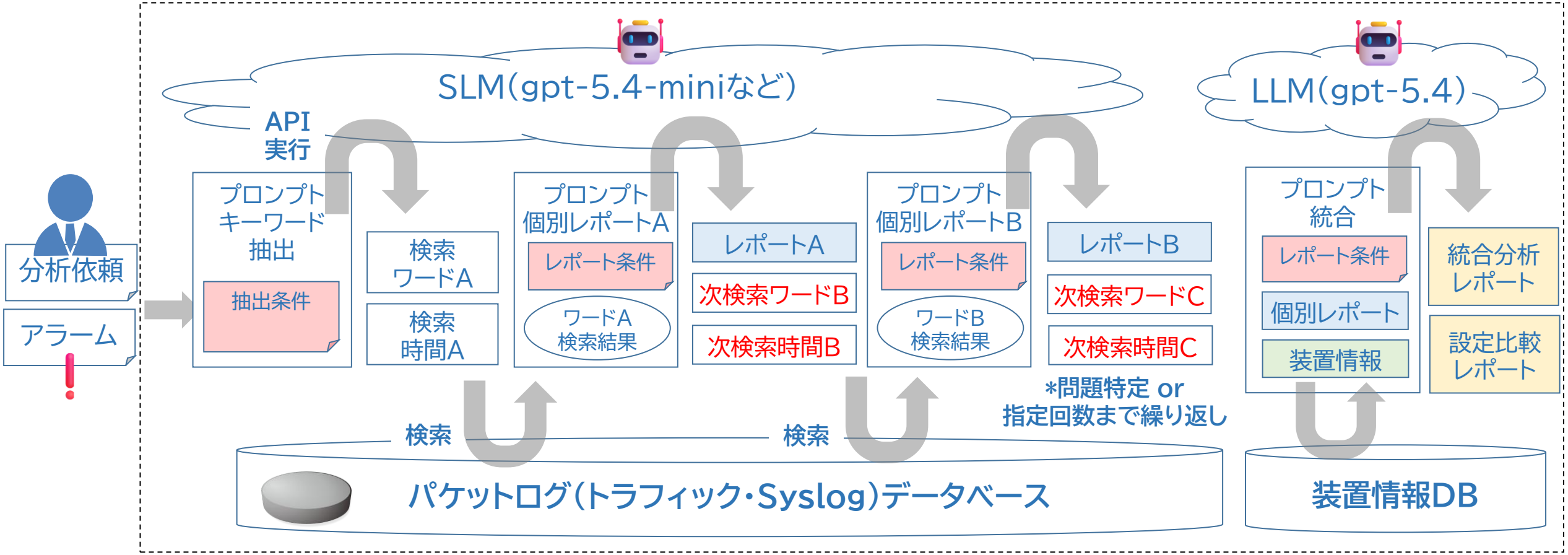




解決策 ： Agent AI による計画的・探索的なログ分析

分析依頼やアラートに合わせて条件を都度変化させる計画・探索型ログ解析

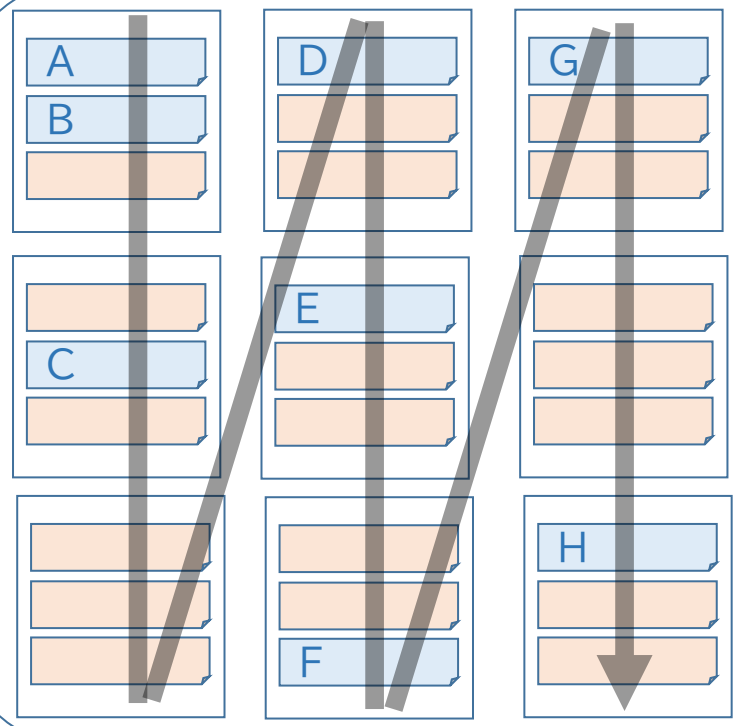
⇒ 検索キーワード・検索件数・検索時間のフィードバックにより、分析精度を向上



Interop Tokyo ShowNet 2026
LLM連携分析例

ShowNetアラーム ＋ LLM連携分析

アラーム発報（分析依頼） → 探索調査 → 探索まとめ → 追加探索 → 結果報告

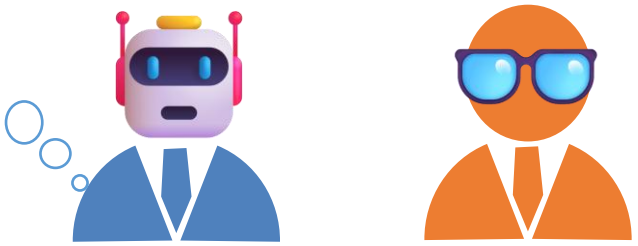


どんな依頼を受けた？

どんなトラブルが発生している？

主原因A	主原因B
補助情報C	補助情報D
補助情報E	補助情報F
補助情報G	補助情報H

（結果回答）



原因を分析して！

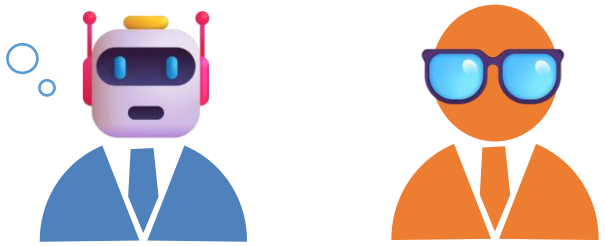
ShowNetアラーム ＋ LLM連携分析(アラーム発報)

アラーム発報（分析依頼） → 探索調査 → 探索まとめ → 追加探索 → 結果報告

どんな依頼を受けた？

どんなトラブルが発生している？

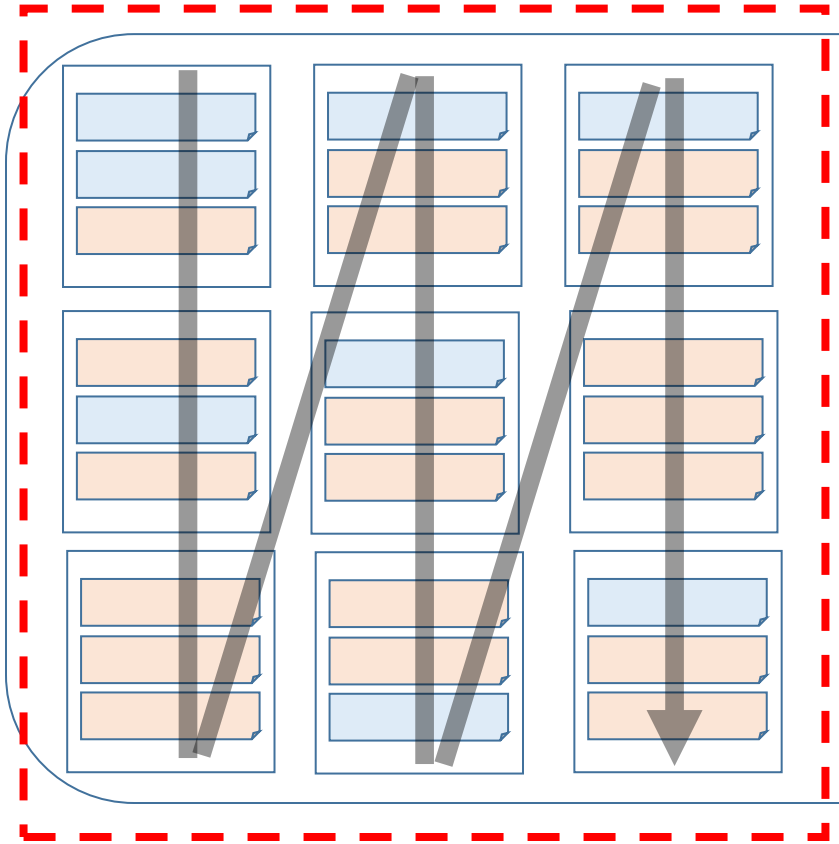
（調査中・・・）



原因を分析して！

ShowNetアラーム ＋ LLM連携分析(探索調査)

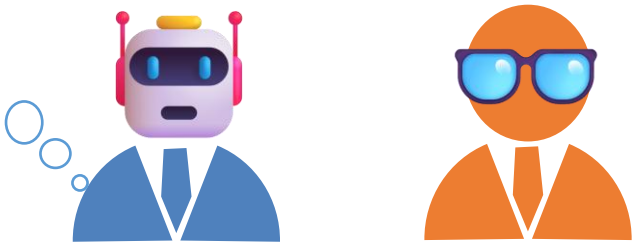
アラーム発報（分析依頼） → 探索調査 → 探索まとめ → 追加探索 → 結果報告



どんな依頼を受けた？

どんなトラブルが発生している？

（分析中・・・）



原因を分析して！

ログ探索調査(1)

```
# GAIPAR Investigation Trace

## User Trouble
Problem:SNMPTrapLinkDownProblem:SNMPTrapLinkDownHostptx10002-36qdd.noc[172.16.0.5]Eventtime2026.06.
1014:31:12SeverityHighOpdata20260610:143112LinkDown[.1.3.6.1.6.3.1.1.5.3]520|up|down|et-0/0/1EventtagsApplication:SNMPTrapTriggerdescription

## Initial Search Plan
- keyword: [["ptx10002-36qdd.noc","172.16.0.5","snmptrap","linkdown","down","up","et-0/0/1"]]
- range: 20260610 1421 - 20260610 1441
- reason: 初回探索。症状の表面を把握する。

## Timeline

### Cycle 1
- search: [["ptx10002-36qdd.noc","172.16.0.5","snmptrap","linkdown","down","up","et-0/0/1"]]
- range: 20260610 1421 - 20260610 1441
- reason: 初回探索。症状の表面を把握する。
- hits: 500189
- samples: 1022
- quality: ok
- sufficiency: insufficient
- should_continue: yes
- decision: continue
- next_action_type: packet_search
- next_keywords: ["link"]
- next_must: ["et"]
- decision_reason: 今回の結果で、ユーザー依頼のSNMPTrapLinkDownに対して対象装[redacted]の14:31:12前後にRPD_IFL_NOTIFICATION(state=UpDown,
et-0/0/1.3204)という整合する補助証拠は得られたが、et-0/0/1自体の物理リンク断を示す直接証拠(IF_DOWN_LINK_FAILURE/LINK-3-UPDOWN/LINEPROTO-5-UPDOWN/
hwPortDown等)は未取得で、原因断定には不足している。次探索では前回の広いsnmptrap/linkdown検索から差分として、同一装置・同一時刻帯のまま対象IF名et-0/0/1に絞
り、物理リンク変化の直接ログを優先して確認する。
```

①アラートと連動して分析開始

②アラート内容から調査開始
まずは広い範囲で関連ログ検索

[Cycle1 検索]
- 検索結果は500000件
- ログを1000件に集約
- 装置ログは確認できた
- リンクダウンログは見えない

⇒検索時間を変化させて、
物理リンク変化確認を提案

ログ探索調査(2)

```
### Cycle 2
- search: [["link"],["et"]]
- range: 20260610 1430 - 20260610 1433
- hits: 683
- next_keywords: ["lldp"]
- next_must: ["et"]
- decision_reason: 今回の結果で、ユーザー依頼のSNMPTrapLinkDownに対して[redacted]のet-0/0/1でSNMP_TRAP_LINK_DOWN/UPとPICD_LINK_UPDOWN/IFD Notifyが時系列整合し、実リンクflap自体は十分確認できた。一方で、ケーブル・対向装置・光/ポート不良・再ネゴシエーション・管理操作のどれが根因かは未確定で、原因断定にはまだ不足している。前回は物理IFの直接証拠が未取得だったが、今回は直接証拠を取得できたため、次探索では同一装置・同一時刻帯のまま対向側やLLDP/neighbor/adjacency系の補助証拠に差分を広げ、原因候補の絞り込みを行う。

### Cycle 3
- search: [["lldp"],["et"]]
- range: 20260610 1431 - 20260610 1432
- hits: 2
- next_keywords: ["neighbor"]
- next_must: ["et"]
- decision_reason: 今回の結果で、ユーザー依頼のSNMPTrapLinkDownに対して[redacted]のet-0/0/1でSNMP_TRAP_LINK_DOWN/UP、PICD_LINK_UPDOWN/IFD Notifyに加えてLLDP_NEIGHBOR_DOWN/UPも時系列整合し、実リンクflapと隣接消失・復帰は十分確認できた。一方で、ケーブル・対向装置・光/ポート不良・再ネゴシエーション・管理操作のどれが根因かは未確定で、原因断定にはまだ不足している。前回はLLDP補助証拠が未取得だったが、今回は取得できたため、次探索では同一装置・同一時刻帯のまま対向側情報やneighbor/adjacency系の補助証拠に差分を広げ、原因候補の絞り込みを行う。

### Cycle 4
- search: [["neighbor"],["et"]]
- range: 20260610 1431 - 20260610 1432
- hits: 3
- next_keywords: [redacted]']
- next_must: ["et"]
- decision_reason: 今回の結果で、ユーザー依頼のSNMPTrapLinkDownに対して[redacted]のet-0/0/1でSNMP_TRAP_LINK_DOWN/UP、PICD_LINK_UPDOWN/IFD Notifyに加えてLLDP_NEIGHBOR_DOWN/UPとRPD_ISIS_ADJUPも時系列整合し、実リンクflapと対向隣接の消失・復帰は十分確認できた。前回はLLDP補助証拠のみだったが、今回は対向装置[redacted]まで得られたため、次探索では同一時刻帯のまま対向側ログへ差分を広げ、対向瞬断か局所ポート問題かの切り分けを進める必要がある。
```

［Cycle2 分析］
Linkのflapを確認
⇒LLDP状態の確認を提案

［Cycle3 分析］
LLDPネイバーダウンを確認
⇒対向装置確認を提案

［Cycle4 分析］
対向装置のホスト名を確認
ISISプロトコルダウンも確認
⇒対向装置ログ検索を提案

ログ探索調査(3)

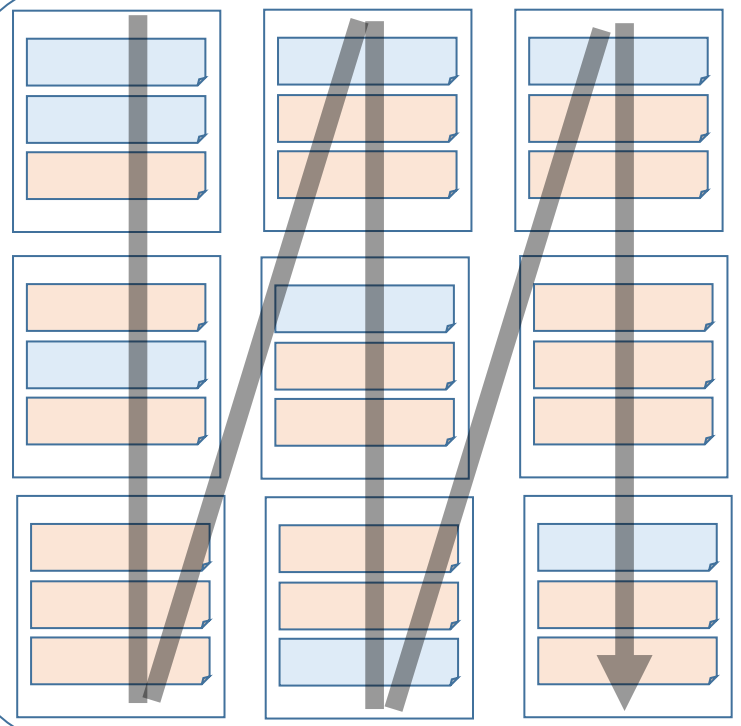
```
### Cycle 5
- search: [["                    :"],["et"]]
- range: 20260610 1431 - 20260610 1432
- hits: 27
- next_keywords: ["link"]
- next_must: ["          ?"]
- decision_reason: 今回の結果で、ユーザー依頼のSNMPTrapLinkDownに対して[redacted]cのet-0/0/1で実リンクflapと対向隣接の消失・復帰は既に確認済みで、今回は対向候補[redacted]:側にも同時刻帯の内部エラー系ログがあることを追加確認できた。前回との差分は『対向装置名の特定』から『対向装置側にも同時刻帯の異常がある』へ進んだ点だが、まだ対向側の該当IFの直接down/upやLLDP/neighborの時系列が取れておらず、対向瞬断か局所ポート問題かの切り分けには不足している。次探索では同一時刻帯のまま、対向装置[redacted]:側でlink/down/upまたは該当IFをさらに絞る検索に進める。

### Cycle 6
- search: [["link"],["          "]]
- range: 20260610 1431 - 20260610 1432
- hits: 42
- decision: stop
- decision_reason: 今回の結果で、ユーザー依頼のSNMPTrapLinkDownに対して[redacted]cのet-0/0/1でSNMP_TRAP_LINK_DOWN/UPとPICD_LINK_UPDOWNが時系列整合し、実リンクflap自体は十分確認できた。以降は原因調査のため、装置情報の確認に移行することが望ましい。
```

［Cycle5 分析］
対向装置ログでも発出を確認
⇒時系列の追加調査を提案

［Cycle6 分析］
時系列でLinkフラップを確認
⇒ログからの調査を終了

ShowNetアラーム ＋ LLM連携分析(探索まとめ)

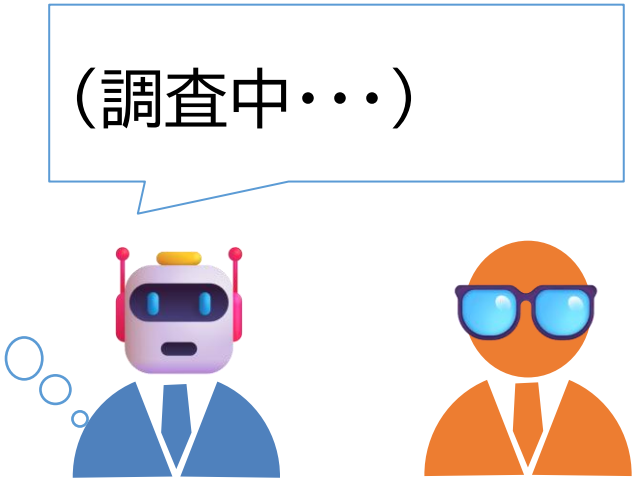
アラーム発報（分析依頼） → 探索調査 → 探索まとめ → 追加探索 → 結果報告



どんな依頼を受けた？

どんなトラブルが発生している？

主原因A　主原因B



ログ探索まとめ(1)

```
# (1) ユーザ依頼文章

`Problem: SNMPTrapLinkDown / Host: [redacted]: [172.16.0.5] / Eventtime: 2026-06-10 14:31:12 / Severity: High / Opdata: 20260610:143112
LinkDown [.1.3.6.1.6.3.1.1.5.3] 520|up|down|et-0/0/1`

---

# (2) 調査方針

- 対象装置 `[redacted]` (IP管理表より [redacted]) の `et-0/0/1` に関するログを中心に確認
- `SNMP_TRAP_LINK_DOWN/UP` と同時刻帯の物理リンク系ログ、論理IFログ、隣接プロトコルログを時系列で相関
- さらに、隣接先としてログ上に現れた対向装置 `[redacted]` (IP管理表より `[redacted]`) の同時刻帯ログを確認
- 調査対象時間は主に `2026-06-10 14:31:00-14:32:00` 周辺

---

# (3) 調査結果

## 要約

`[redacted]` の `et-0/0/1` では、**2026-06-10 14:31:12 前後に実際のリンク変動（短時間 flap）が発生**しており、発報された `SNMPTrapLinkDown` はその実イベントと整合していました。
加えて、同インタフェース配下の論理IF、LLDP隣接、IS-IS隣接にも時系列整合する変化が確認されました。

一方で、**根因を一意に特定できるログ（ケーブル不良、光モジュール不良、保守操作などの直接証拠）は確認できていません。**
```

[調査方針まとめ]
・SNMPTrapを受けての調査方針
・どういった観点で分析を行ったか

[調査結果要約]
・短時間Flapが発生している
・隣接IFでも同様の問題あり
・ケーブル不良等の証拠はない

ログ探索まとめ(2)

総合評価

調査達成度：中〜高（事象確認は十分、根因特定は未達）

- **十分確認できた点**
  - 対象IF `et-0/0/1` のリンク flap
  - trap と syslog内容の時系列整合
  - 論理IF・LLDP・IS-IS への波及
- **未確定な点**
  - 根因が局所ポート要因か、対向要因か、物理媒体要因か
  - 対向側 [redacted] の該当IFにおける直接的な down/up 記録
- **妥当な結論**
  - 本件は [redacted] の `et-0/0/1` における**実リンク flap 事象**
  - ただし、**根因は追加ログまたはコンフィグ照合なしでは断定不可**

ログ調査対象機器

優先度	IPアドレス	hostname/装置名	役割	関連する事象	調査対象とする理由	確認すべき観点
高	[redacted]	[redacted]	router	`et-0/0/1` の SNMPTrapLinkDown、物理リンク flap、LLDP/IS-IS 隣接変化	全サイクルで中心となった対象装置であり、物理IF・論理IF・隣接変化の主要ログが集中しているため	interface, optics, transceiver, errors, lldp, isis, syslog
高	[redacted]	[redacted]	router	対向候補として IS-IS 隣接再確立、同時刻帯の packetio/evo-cda-bx エラー	[redacted] 側ログで対向候補として特定され、同時刻帯に関連ログがあるため、片側要因か対向要因かの切り分けに必須	interface, errors, lldp, isis, optics, transceiver
中	-	et-0/0/1 ([redacted]上)	interface	物理 link down/up、trap発報元インタフェース	原因が機器全体ではなく該当物理IFまたは配下論理IF起因の可能性があるため	interface, counters, flap-history, optics
中	-	et-0/0/29.0 [redacted]上)	interface	`RPD_ISIS_ADJUPNOIP` に現れた対向候補IF	`et-0/0/1` に対向する可能性が高く、対向側直接証拠の確認対象となるため	interface, lldp, isis, counters, flap-history

［探索結果評価］
・確認できたのはリンクのflap事象
・時系列でログとの整合性も確認
・原因特定までは至っていない
⇒ コンフィグ照合やログ追加が必要
※追加調査対象機器の抽出

ログ+構成図+装置コンフィグの探索的分析(1)

NTT AT

コンフィグ照合レポート

1. 結論
- **設定起因の可能性：低**
  - `[redacted] et-0/0/1` と `[redacted] et-0/0/29` の対向設定は、主要項目で**概ね対称かつ整合**しています。
  - 少なくともコンフィグ上では、`disable`、速度不一致、VLAN不一致、encapsulation不一致、IS-IS不一致、LLDP無効化差異など、**リンク flap を直接誘発しやすい明確な設定不整合は確認できません**。
  - finalレポートのとおり、事象自体は実リンク変動ですが、**根因はコンフィグよりも物理層/光/モジュール/対向装置側ハードウェア・PFE要因の方が疑わしい**です。
- **補足評価：中**
  - `[redacted]:` 側で同時刻帯に `packetio` / `evo-cda-bx` のエラーログがあり、完全に設定要因をゼロ断定はできません。
  - ただし、これらを説明する**明白な設定ミスは今回のコンフィグ照合では見当たりません**。
- **高とはしない理由**
  - 影響インタフェース双方で、速度・波長・appselid・VLAN 104・CCC VLAN群 3200-3204・IS-IS有効化が揃っており、恒常的な設定不整合なら継続障害になりやすいところ、本件は**短時間 flap**です。

---

2. 確認対象装置
hostname	config有無	確認理由	優先度
[redacted]	有	発報元。`et-0/0/1` で物理 flap、論理IF変動、LLDP/IS-IS変動が集中	高
[redacted]	有	対向候補。`et-0/0/29.0` でIS-IS再確立、同時刻帯に packet/PFE系ログあり	高
[redacted] / et-0/0/1	主要装置config内で確認	発報対象IF。物理/論理/L2circuit/IS-IS/LLDP整合確認が必要	高
[redacted] / et-0/0/29	主要装置config内で確認	対向IF。左右対称性、光学設定、論理IF、IS-IS整合確認が必要	高

[コンフィグ照合結果]
コンフィグ設定は問題がないことを確認

[調査対象機器]
コンフィグ等の情報が取得できた装置

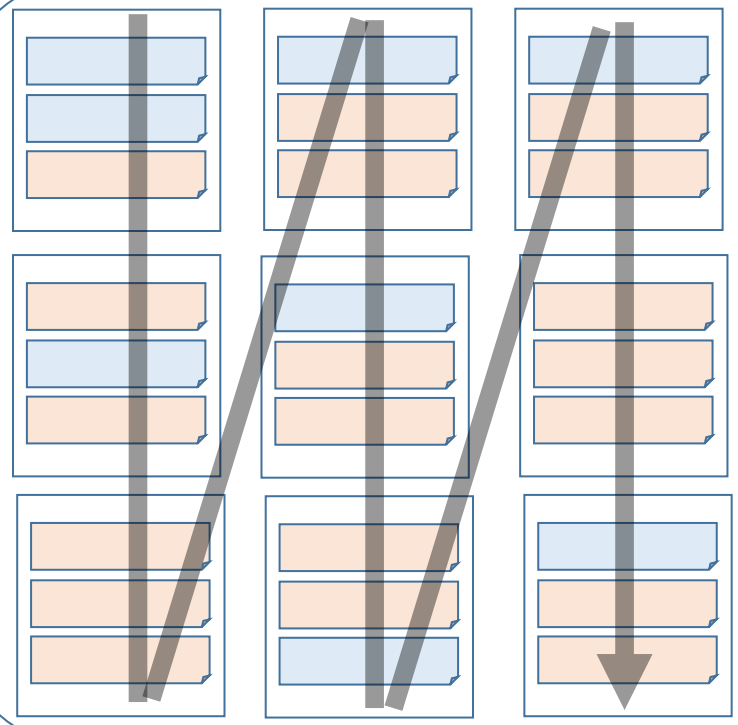
ログ+構成図+装置コンフィグの探索的分析(2)

```
## 5. 未確認・不足情報
- **光学/物理層の実測値**
  - Tx/Rx power
  - laser bias/current
  - module temperature
  - BER / FEC / PCS / MACsec有無 / lane error
- **IF flap履歴**
  - flap回数、継続期間、直近増加傾向
- **対向の直接物理down/upログ**
  - finalレポートでは 60mr 側に明示的な物理 link down/up が不足
- **コミット履歴の詳細**
  - 事象直前にIF関連設定変更があったか
- **既知不具合情報**
  - [redacted] / 26.2 EVO 間、800G optics、CDA/PFEログに関するPR/既知事象
- **回線情報**
  - 中間のMUX/OTN/DWDM有無、パッチ変更、保守作業有無
- **エラーカウンタの時系列**
  - CRC/FCS, giants, code violations, local/remote fault
```

[追加調査情報]
- 光のパワー(Tx / Rx)
- 設定変更履歴
- 既知不具合情報
- 回線情報(保守作業など)
- エラーカウンタ

ShowNetアラーム ＋ LLM連携分析(分析結果報告)

アラーム発報（分析依頼） → 探索調査 → 探索まとめ → 追加探索 → 結果報告

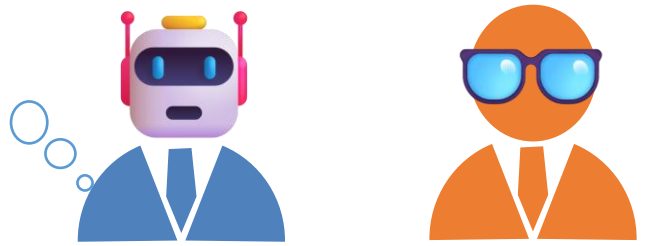


どんな依頼を受けた？

どんなトラブルが発生している？

主原因A	主原因B
補助情報C	補助情報D
補助情報E	補助情報F

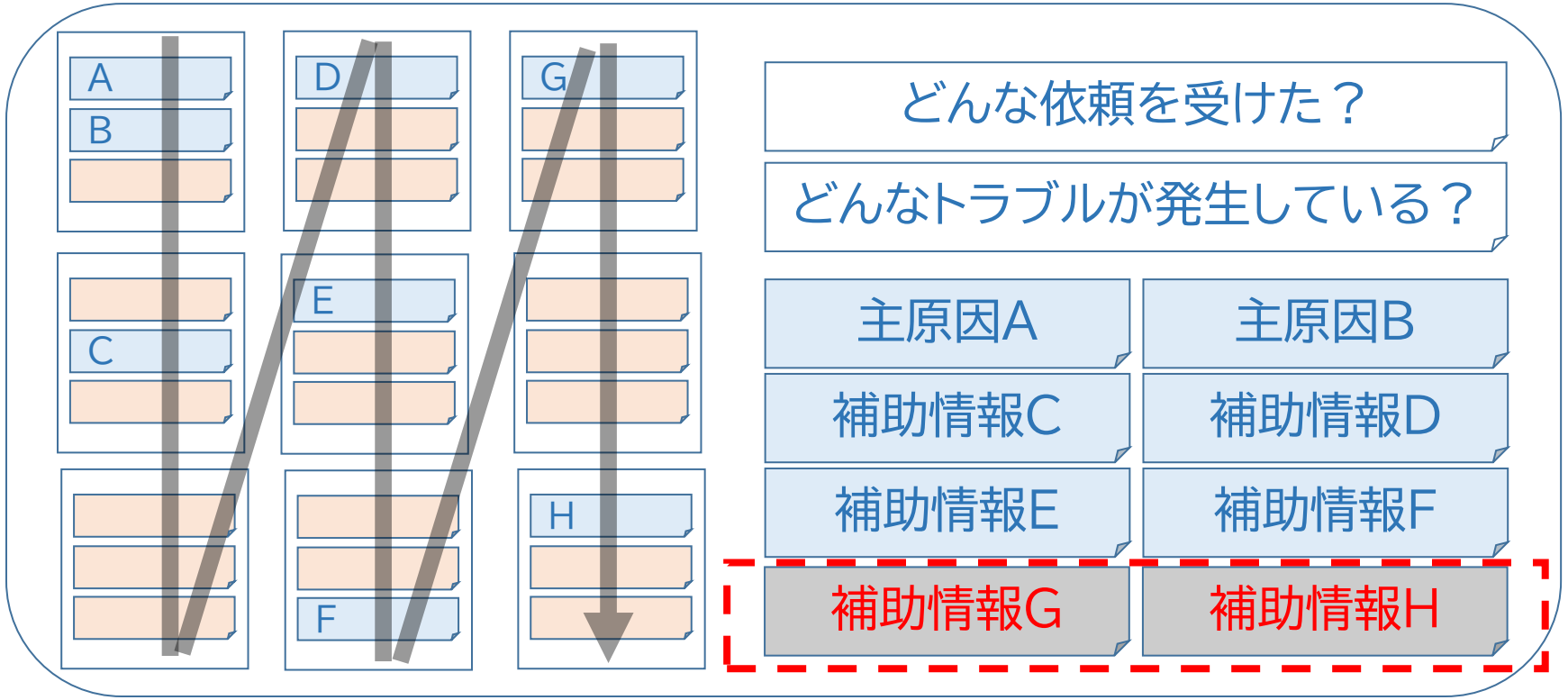
物理的断が原因
光学/物理層を見て

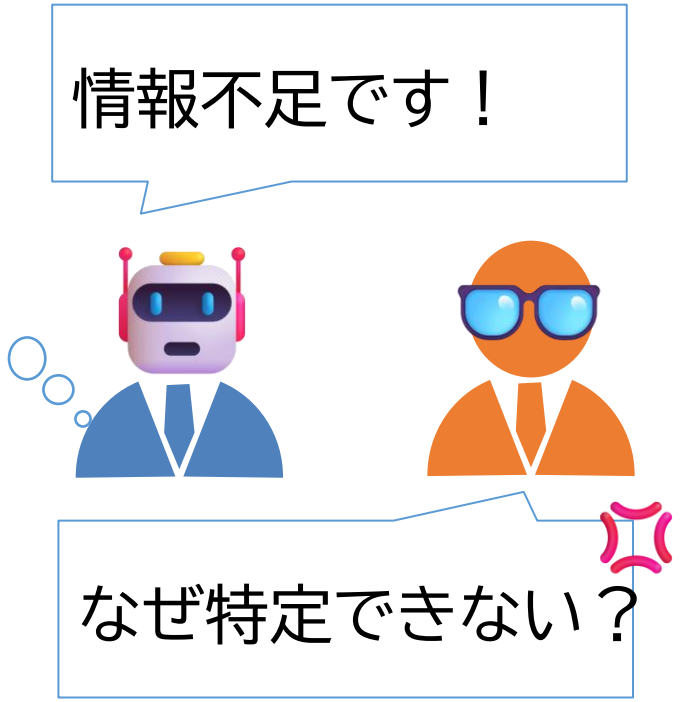


原因を分析して！

LLMオペレーションの完全自動化に向けて

追加の補助情報を収集できれば、同じ仕組みで分析精度はより向上する
⇒ LLMによる完全トラブルシューティングは、延長線上に存在する！

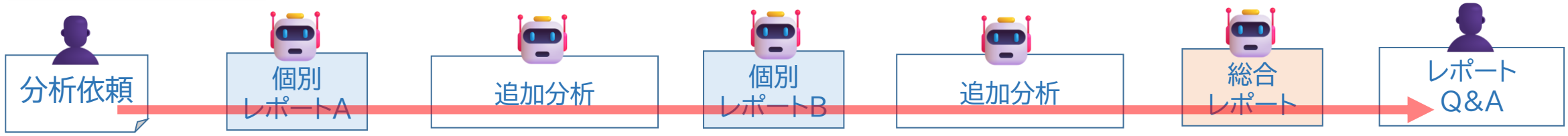




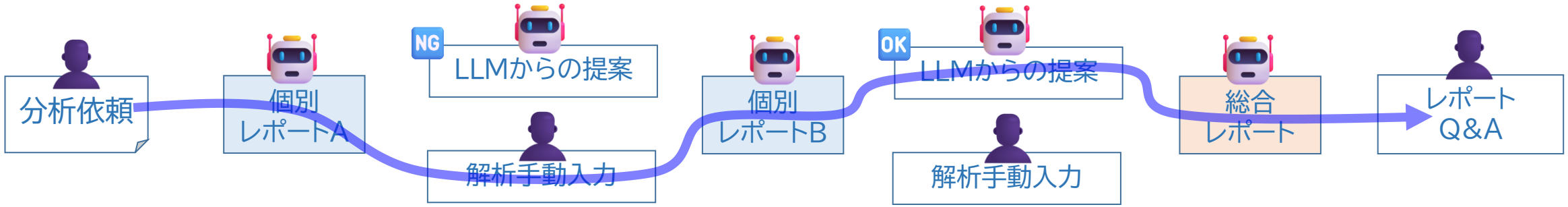
「LLMに任せる」か「LLMと一緒にやる」かの選択

ユーザーの利用目的に合わせて、LLMのサポートレベルを使い分けられるように
⇒ 手動分析はLLM協力型で、アラート連携などはLLMおまかせで実行させる

LLMおまかせ分析 ： LLMが計画・分析・追加分析までを、まとめて実行



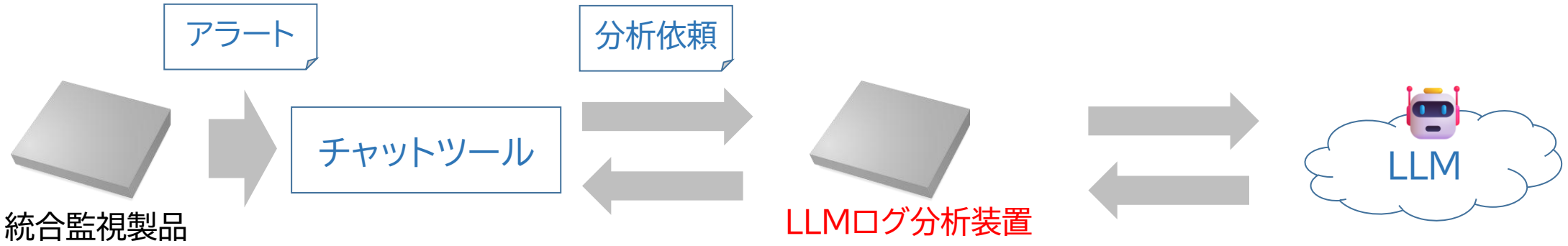
LLM協力型分析 ： LLMの分析結果・次の分析提案をオペレーターが修正しながら実行

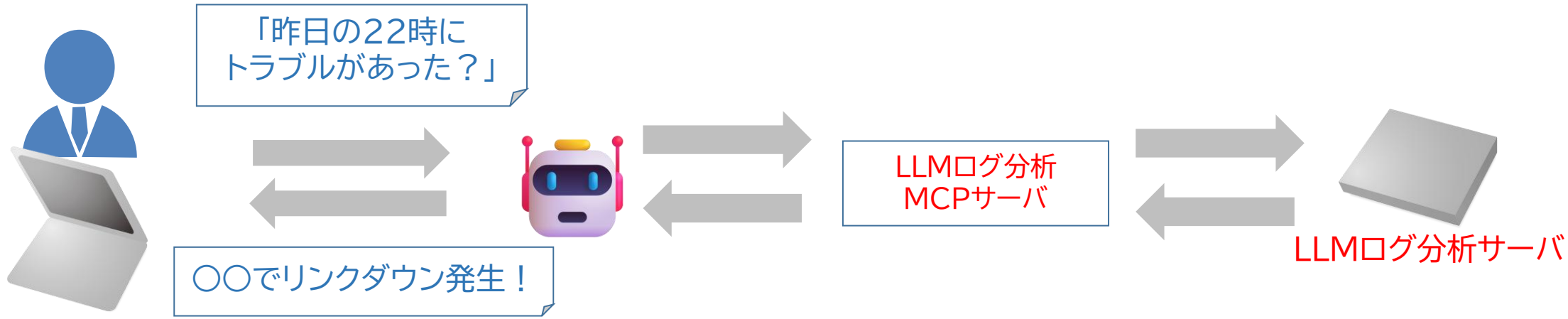


MCPを活用したネットワーク監視の外部連携実証(1)

アラート連携で蓄積したレポートをMCPサーバで提供

アラートをトリガに常時分析





MCPを活用したネットワーク監視の外部連携実証(2)

分析例　入力　～　MCP tools/callで過去のレポートを解析

```
> MCPサーバを使って2026年6月9日の22時から23時のshownetのネットワークを分析してください。最初のステップではflowinspectorのMCPを利用して分析をスタートしてください。

· shownet の 2026年6月9日 22:00-23:00 を対象に、まず flowinspector の MCP ツールを特定して調査を開始します。最初に使える flowinspector 系ツールと対象データへの入口を確認します。

· flowinspector ではまず該当時間帯の統合レポート一覧を引きます。ここで 22:00-23:00 の粒度と利用可能なレポートを確認し、その後に必要なら他の MCP を補助的に使います。

· Called flowinspector.get_report_lists({"start":"2026-06-09 22:00:00","end":"2026-06-09 23:00:00"})
  └ ===== 2026-06-09 22:05:13 (20260609_220513/gpt_result_Summary_report.md) =====
    # 統合レポート

    ## (1) ユーザ依頼文章

    `SNMPTrapLinkDown` が発生した原因を調査する。
    対象は                                イベント時刻は `2026-06-09 22:05:11`。
    `Ethernet1/3/1` に関する `up -> down` と `LinkDown` の関係を含めて確認する。

    ---

    ## (2) 調査方針

    1. 初回は `SNMPTrapLinkDown` 周辺の trap 送信ログを確認し、同時刻帯での反復有無を確認する。
    2. 次に対象IF `Ethernet1/3/1` の状態変化ログを確認し、trap と時系列整合するかを確認する。
    3. 追加で `hwPortDown`、`LLDP`、`physical`、`port` などの補助証拠を探索し、根本要因の裏付けを試みる。
    4. 調査評価は、以下の客観的指標で行う。
       - 対象IFの状態変化ログ有無
       - trap 時刻との時系列整合性
       - 物理断・対向消失を示す補助証拠の有無
       - 同時間帯での再現性

    ---

    ## (3) 調査結果

    ### 3.1 主要な確認結果

    個別レポートを通じて、以下が確認できた。
```

link downのアラートが
22:00-23:00に存在

MCPを活用したネットワーク監視の外部連携実証(3)

分析例　アラートも合わせて分析し、最後に結論を推測する

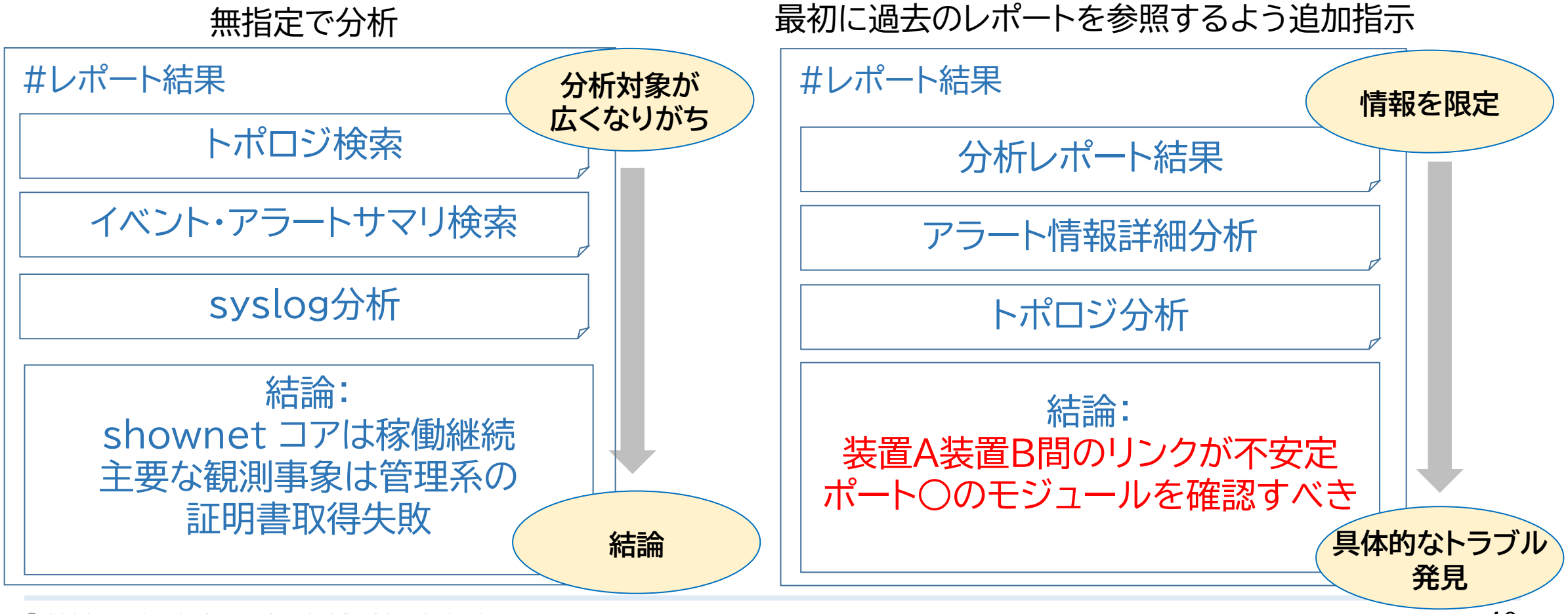
```
· 2026年6月9日 22:00-23:00 の shownet について、まず flowinspector の統合レポート一覧を確認し、その時間帯の事象を整理しました。追加で                    のアラートも見ましたが、監視アラートは
  timeout/recovery が少数あるだけで、1時間全体の広域障害を示す材料は出ませんでした。

  この1時間で支配的だったのは、特定 2 台のリンク不安定化です。

  1.
     Ethernet1/3/1 で IF_DOWN_LINK_FAILURE と IF_UP が 22時台を通じて反復しており、少なくとも 22:00:02、22:02:37、22:05:10、22:07:44、22:10:19、22:23:09、22:35:59、22:51:23、22:53:56、
     22:56:31 付近で down 系イベントが確認できます。22:37:18 には speed/duplex/flow control の再交渉を伴う IF_UP も見えており、単発断ではなくフラップ傾向です。
     ただし、この機器では hwPortDown や LLDP の補助証拠が乏しく、原因は「リンク断系」までは言えても、ケーブル・光・対向・ポート内部のどれかまでは確定できません。

  2.
     800GE1/0/3:1 で、こちらはより強い証拠が出ています。22:16:41、22:41:25 などで hwPortDown、22:42:40 などで hwPortUp、同時に LLDP neighbor deleted/added、さらに 22:45:30、22:49:35、
     22:53:41 付近で linkDown active が出ており、Reason=Interface physical link is down まで確認されています。対向は                              /                  と読めます。
     この系統は、物理リンク断を伴うフラップと判断してよい状態です。

  全体所見として、この 1 時間の shownet は「ネットワーク全体が広く落ちた」というより、DC 側の特定リンク 2 系統で断続的な linkDown/linkUp が継続していた時間帯でした。特に                  側は物
  理断の確度が高く、                側も同種のリンク不安定化が濃厚です。
  したがって、この時間帯の優先調査対象は次の 2 点です。

  -            800GE1/0/3:1 と対向                の物理層
  -            Ethernet1/3/1 の対向ポート、光モジュール、ケーブル、エラーカウンタ

  必要なら次に、              と                を中心に「5分単位の障害タイムライン」か「対向関係を含む影響範囲表」まで掘ります。

> この結果をもとに、報告用のレポートをmdファイルで作成してください。

· 分析結果を報告用の Markdown に整理し、                配下にレポートファイルを作成します。見出しと要約、主要事象、評価、次の調査観点まで含めた提出向けの体裁にします。

· 報告用レポートを作成しました。ファイルは shownet_analysis_report_2026-06-09_2200-2300.md です。

  内容は、分析方法、全体所見、              と                の主要事象、結論、追加確認事項まで含めた提出向けの構成にしています。必要なら次に、これを「社内報告向けの短縮版」か「障害報告書フォー
  マット」に合わせて整形します。
```

この1時間では2台のリンクフラップが発生していたという結論

MCPを活用したネットワーク監視の外部連携実証

事前にアラート連携でナレッジを貯めることでより効率的に分析

「MCPサーバを使って2026年6月9日の22時から23時のshownetのネットワークを分析してください。」



結局、いくらかかったのか？

実証期間における分析コストサマリー

※ Interop ShowNetで実際にかかった金額は、
プログラム講演時にご紹介させていただきます。

大規模ネットワーク2026における運用結果まとめ

期間中の大規模NWログ分析では、以下の結果となった

前提 ： ログ分析にSLM、統合処理にLLMを使用

- アラート分析によるコストは2週間で約XX万円
- 1回あたりの分析実行には約XX円

「安い」と思いますか？「高い」と思いますか？

実サービスにおけるコスト事例

どのようにサービス提供した(している)か？

提供形態

- 分析機器(ミニPCやサーバ)の貸し出し
- 年間サブスクリプション(定額制)

利用方法

- チャット形式での分析実行
- 定期実行形式での分析実行

※ともに、LLMの回答結果内容のサポートはしない

実利用コスト ： トークン課金の状況

※ 実サービス運用で実際にかかった金額は、
プログラム講演時にご紹介させていただきます。

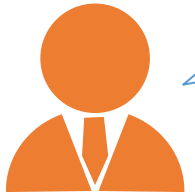
なぜ「利用金額」が想定より高くなったのか？

Q. なぜ利用金額が想定より高くなってしまったのか？

A. サブスクなら / 使ってしまおう / LLM

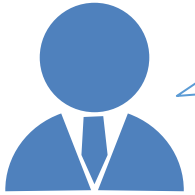
「定額制なら動かしておきたくなる」がコストに直結する

想定：



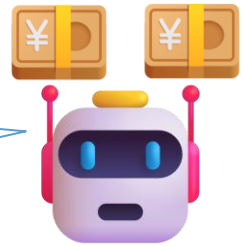
トラブルシューティングが頻発するヘビーユーザーは多くない。
手動実行が中心だから、ライトユーザーが大多数になるはず。

実態：



目立ったトラブルはないけど、
監視のためにとりあえず毎時レポート出しておこう！

（日々の通信や傾向をまとめた”定期分析レポート”を作成）



コスト面で見た際のLLMオペレーションとの競合

Case1．イベントドリブンによるトラブル解析
⇒　ログ探索/検索の回数や期間が限定的

Case2．手動のトラブルシューティング
⇒　回数や期間は変動するが、あくまで手動実行

Case3．LLMによるログ定時監視
⇒　時間単位で必ずトークン数を消費してしまう

有力なユースケース

費用を含めた「LLM利用フロー」を設計しよう

分析は出来る、だが利益を生まないでは当然ダメ

- ネットワーク運用でLLMを使用する場合
- LLM分析をサービスとして提供する場合

上記いずれにおいても、
目的と用途に沿ったLLM費用設計が最重要となる
※ 削減コスト ＜ 利用コストになったら意味がない！

LLMオペレーションにおける利用コスト

LLMをオペレーションに使っていくためには

「LLMのNWオペレーション適用」における”コスト”要素とは？

（1） イニシャルコスト

（2） ランニングコスト

LLMの利用パターンと実行方法

LLMを利用する方法は大きく分けて2種類
その実現方法によってイニシャル・ランニングコストは異なる

#	利用パターン	実行方法
①	外部API利用	OpenAIなどのクローズドモデル AWS Bedrockなどのオープンモデル実行
②	ローカルLLM利用	オンプレサーバ(+GPU)実行 インスタンス(+GPU)実行

LLM利用における「イニシャル」と「ランニング」

イニシャルコストを重要視するか、ランニングコストを重要視するか？

○ イニシャルコスト

#	サーバ費(性能要件)	GPU費
①	ミニPC or デスクトップPC級	不要
②	タワーPC or IAサーバクラス級	ほぼ必須(TPS面など)

○ ランニングコスト

#	トークン費用	使用電力費	モデルアップデート稼働
①	従量課金	低い	エンドポイント変更
②	なし	高い	ローカルモデル変更

赤字:比較して優れている点

イニシャルコスト・ランニングコストまとめ

① 外部API利用
⇒ 導入は安く、運用はトークン従量課金で高め

選択中

精度も高いし、どんどんモデルも自動でアップデートするし…

② ローカルLLM利用
⇒ 導入は高く、運用はトークン利用が定額制となり安め
ただし、電力やモデルアップデート費用の考慮も必要

#	利用パターン	イニシャル	ランニング
①	外部API利用	安い	高め(主にトークン利用)
②	ローカルLLM利用	高い	安め(電力費など含む)

そんなに単純ではない！

イニシャル・ランニングコストだけではない「コスト」とは？

LLMオペレーションは、精度や費用ではない越えられない壁が存在する

○　セキュリティリスク

#	利用パターン	モデルデータ学習	データリージョン
①	外部API利用	オプトアウトで回避	国外のみのモデルあり
②	ローカルLLM利用	なし	国内・ローカル

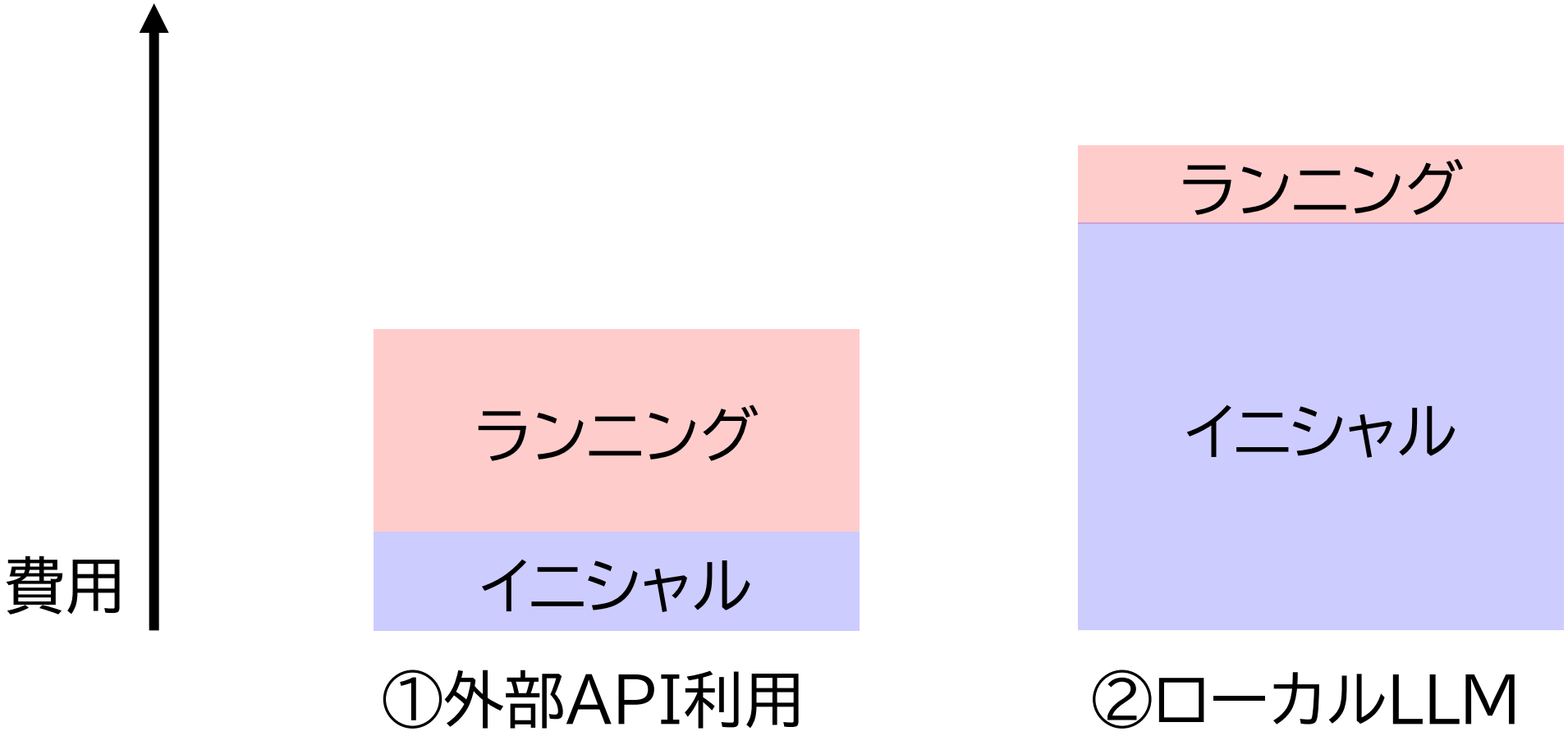
○　グローバルリスク

#	利用パターン	技術輸出管理	ガバメントリスク
①	外部API利用	要調査・要考慮	モデルの提供停止
②	ローカルLLM利用	不要	ない

赤字：比較して優れている点

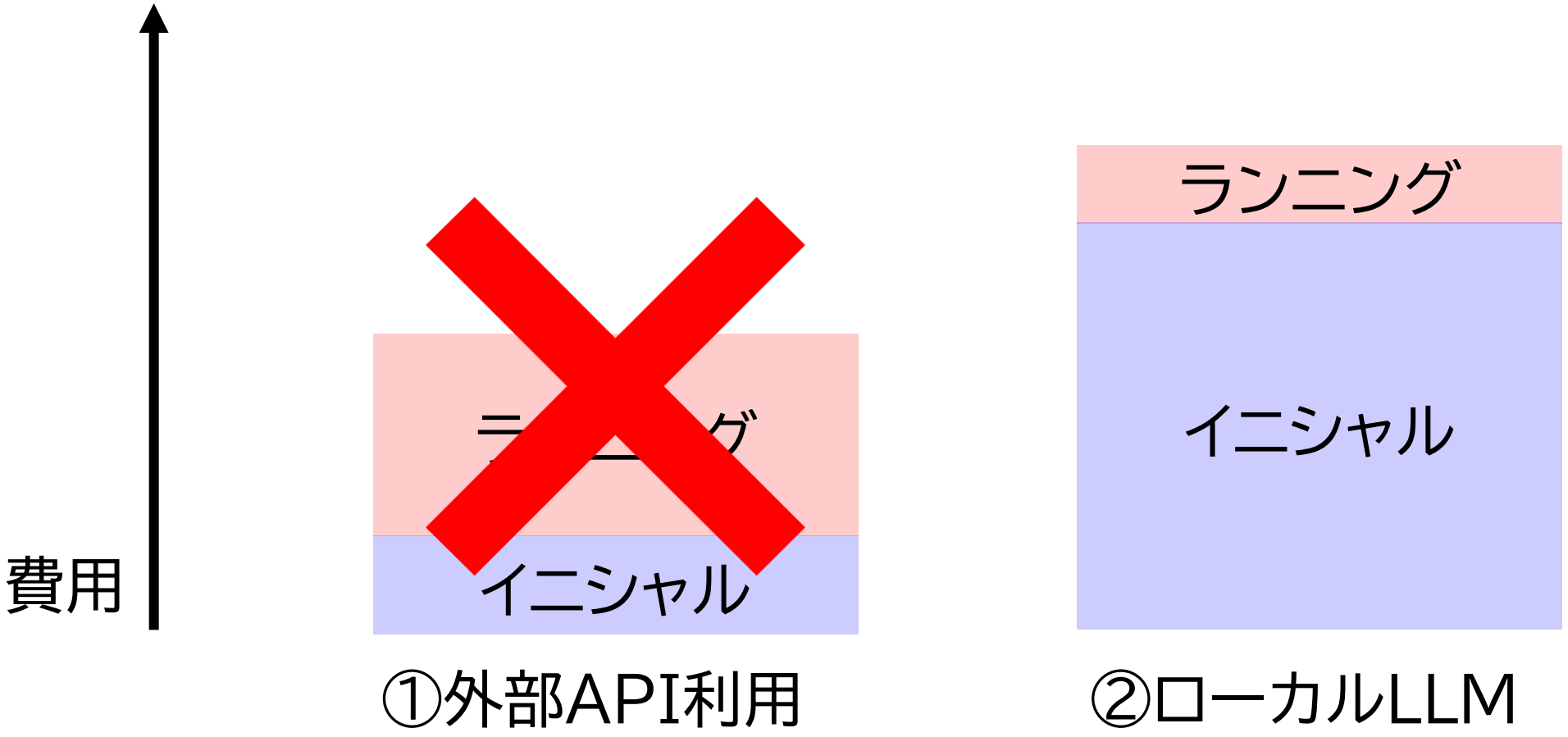
理想

ランニングは高めだが、精度も高い①外部API利用をしたい！



現実(1)

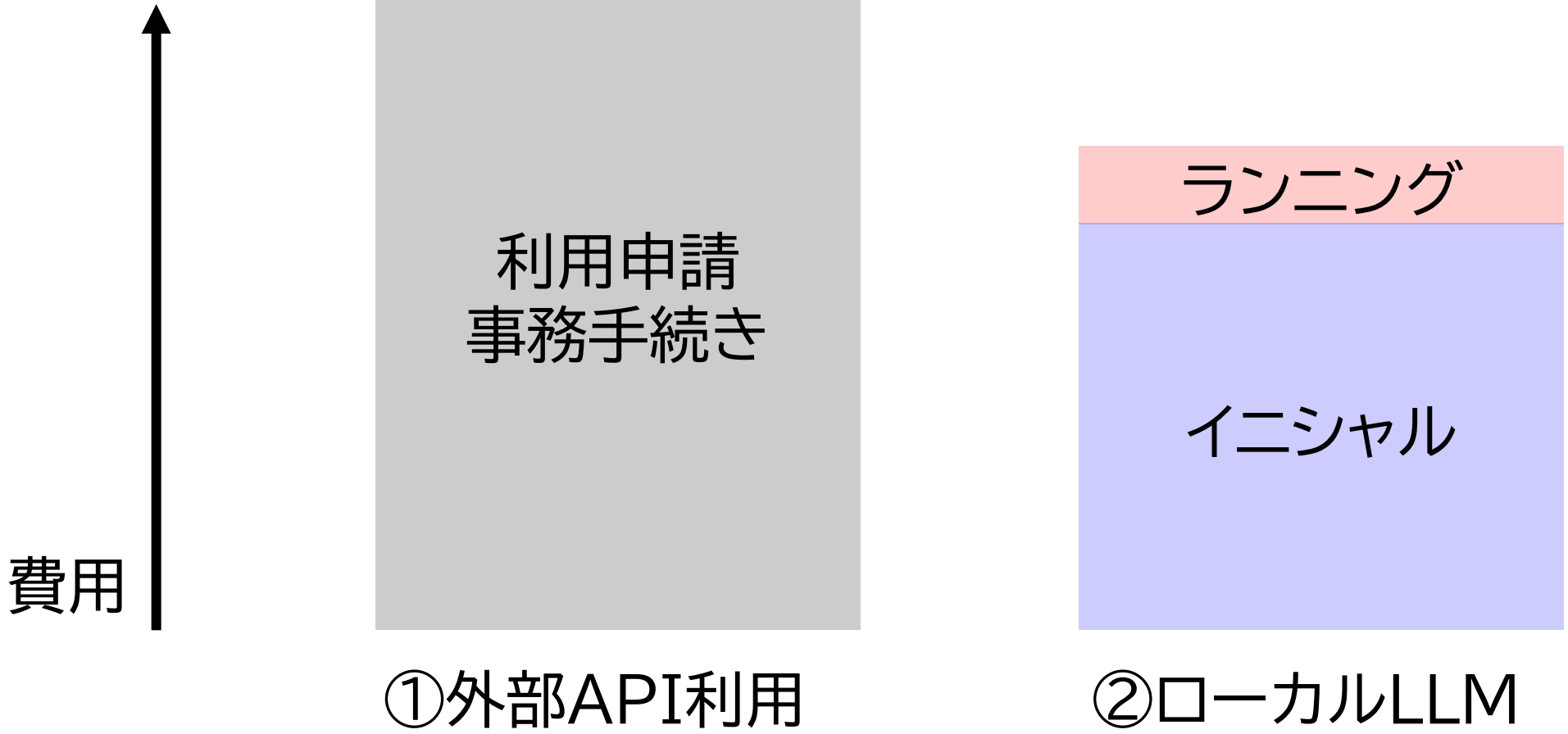
「データは学習に使用しない」と言われてもダメなものはダメ



現実(2)

利用までの

手続きに時間がかかりすぎる



費用を含めた「LLM利用フロー」を設計しよう

精度やトータルコスト(従量を加味しても)を考慮すると、
プロプライエタリな外部APIが採用されがちだが・・・

- トークンコストの変化
- 情報セキュリティの方針
- 不測の事態によるモデル提供停止

に備え、「ローカル」は常に備えておく必要がある

オープンモデルLLMの展望と利用コスト

オープンモデルの進化

3年間で、単なる遊びや実験の段階から　→　実用可能なものに

2023年

Llama2, Mistral 7B
がSLMの能力を示した

2024年

Llama3、Gemma等が
中堅クローズドモデルに
追いかけた

2025年8月

OpenAIの初オープン
モデルがリリースされた
gpt-oss-20b/120b

2026年

MaaS　プラットフォーム
（Bedrock、Vertex）にて
様々なオープンモデルを提供

■ メリット（gpt-oss-20bを例として）

① Apache 2.0等の
オープンライセンス

② ~16GB VRAMの
1 GPUで動かせる

③ クラウドサービスも安い
インプット: $0.07/1M

どのようなタスクに向いているか

処理手順が定期化されている、反復的なタスクに適している
ログ分析： タスクはいつも同じ、変わるのは量だけ

■ ログ分析タスク

- 入力形式は固定： ログ文の構成やエラーコードの意味は変わらない
- 使われる単語・用語もほぼ固定
- 入力データは構造化されている
- 処理件数は多い一方で、1件あたりの価値はそれほど高くない

■ SLMの特徴

- 求められるのは推論力ではなく；パターン認識、異常を見つけること
- エッジ提供： ログを保持している社内環境で動作する； レイテンシ↓ 可用性↑
- 分野をある程度限るとクローズド vs オープンモデルの差が低くなっていく

SLM vs LLM

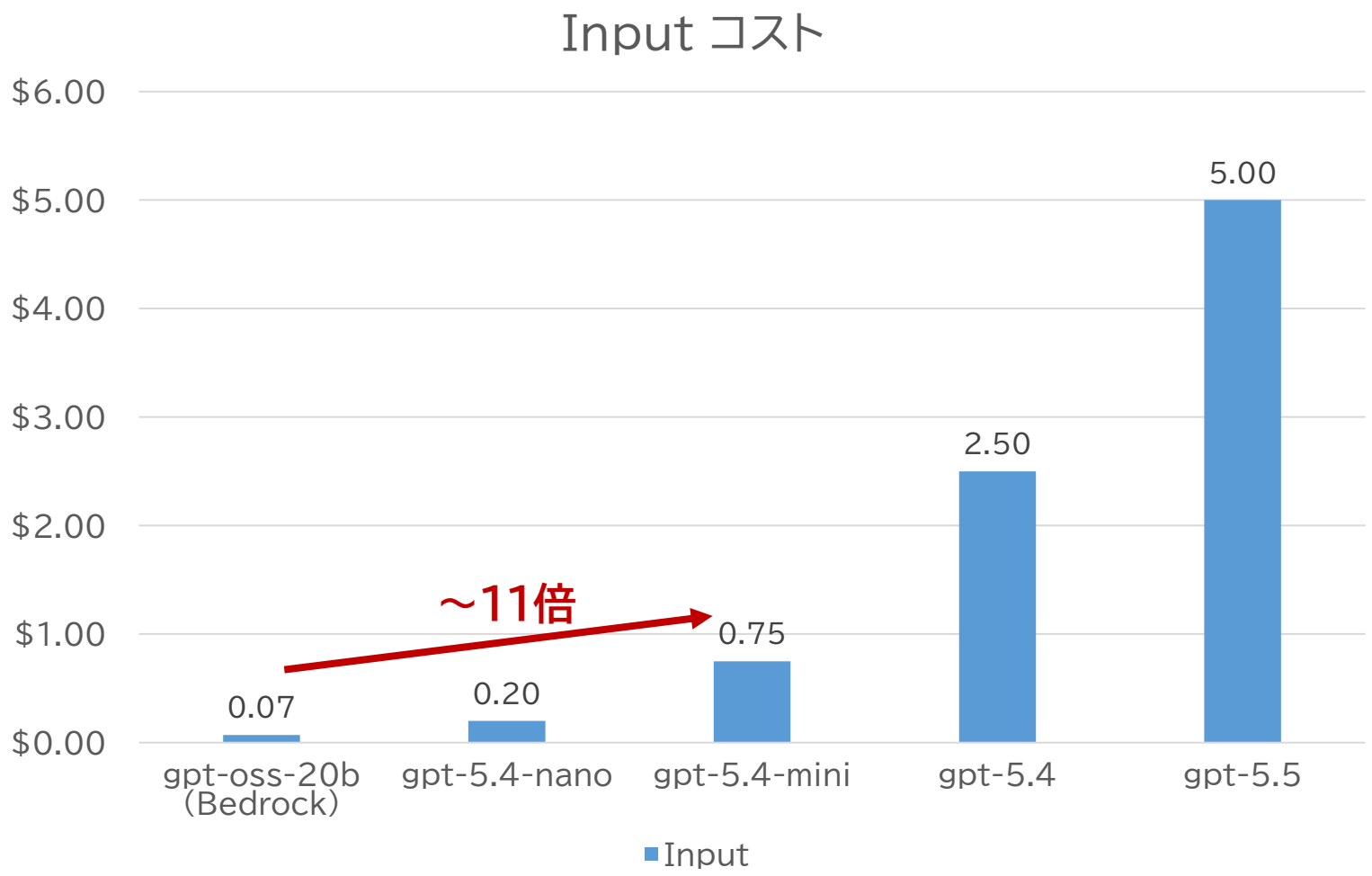
■ SLMで対応できるタスク

- 限定的で、大量に繰り返されるタスク
- 入出力形式は明確に定義されている
- トークン数を大量に使う低価値タスク
- センシティブなデータを取り扱うタスク
- ミスの影響はそれほど高くないタスク

■ LLMが必要になるタスク

- 明確に定義されていないタスクや複数の分野・ドメインをまたがるタスク
- 高品質・精度を求めるタスク
- 少量でも、高価が高いタスク
- 非常に多いコンテキスト量を求めるタスク

トークンコストは？



- Outputコストは、～4-6x
  - gpt-oss: $0.07/0.3
  - 5.4-mini: $0.75/4.5
- ログ分析では：Inputが圧倒的に多い
  - 50K入力ログ文 vs ～2Kトークンのレポート
- 同じタスクに対して：
  - gpt-ossのコストは5.4miniの～9%

基本パイプライン

大量のログファイルを分析し、中間レポートを生成
中間レポートを基に、LLMが判断し、最終レポートを作成

1 ファイル：～50Kトークン

分析する毎度、数十ファイル
を処理する

各ログファイルを分析し、中間
レポートを作成：～2Kトークン

～25:1 トークンを圧縮

全ての中間レポートを解析し、
最終レポートを作成する

LLMへの入力は～96%削減

SLMが大量の生ログを分析してくれるので、
コストの高いLLMは、～4%のトークンしか処理しない

3つのコストプラン

1タスク　＝　50K入力トークン、2K出力トークン　で計算すると

■ プロプライエタリ版API

gpt-5.4-mini

$0.047 / タスク

- 1M トークン毎に：
  $0.75/$4.50
- 高品質、インフラ不要
- データはクラウドにアップされる
- モデルが使えなくなる or
  コストが上がるリスクあり

■ マネージドサービスAPI

gpt-oss-20b (Bedrock)

$0.0041 / タスク

- 1M トークン毎に：
  $0.07/$0. 30
- ～11x安い、インフラ無し
- 特別プランでより安くなる
- クラウドにデータアップロード
  されることは変わらない

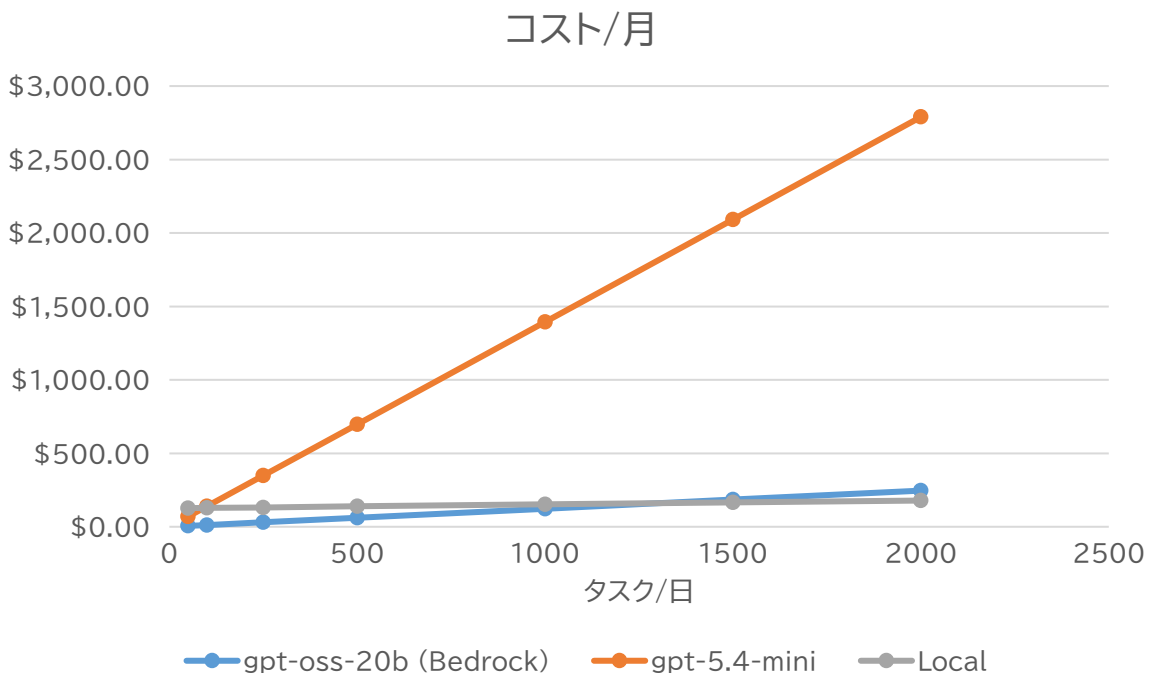
■ ローカル環境

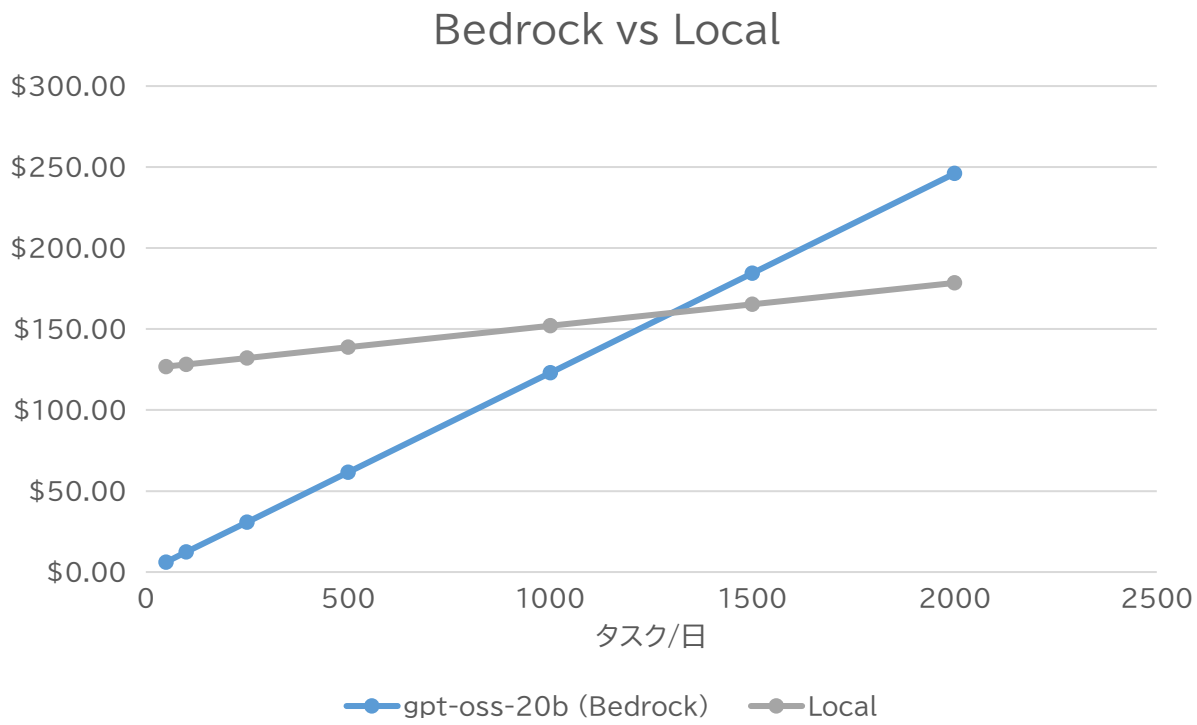
gpt-oss-20b

＜ $0.001 / タスク

- ～4000$の設備投資、
  後は電気代のみ
- 3年間償却：～125＄/月
- データはいつもローカルで
- 環境メンテナンス負担はある

コストの区切り点





- 最初から、BedrockはOpenAIのAPIより安い
- ～100タスク/日の段階で： OpenAIのコストより、ローカル設備投資の勝ち
- ～1400タスク/日まで： BedrockのAPIを使うのがコスパ的に良い

コスト削減は「条件付き」

ここまでの話しは： 精度基準を満たすことを前提としている
公開ベンチマークで検証はできない

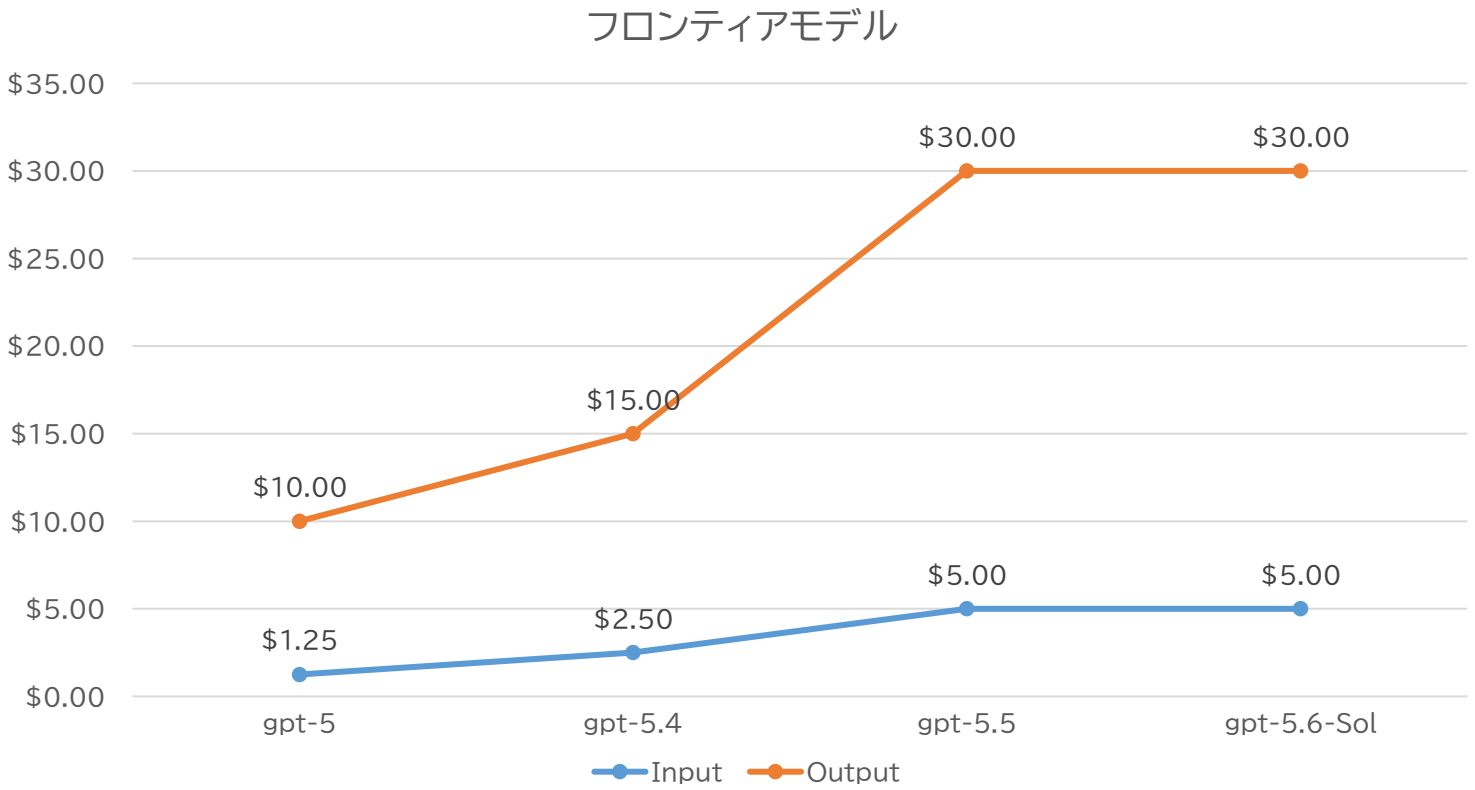
■ 導入前に検証を

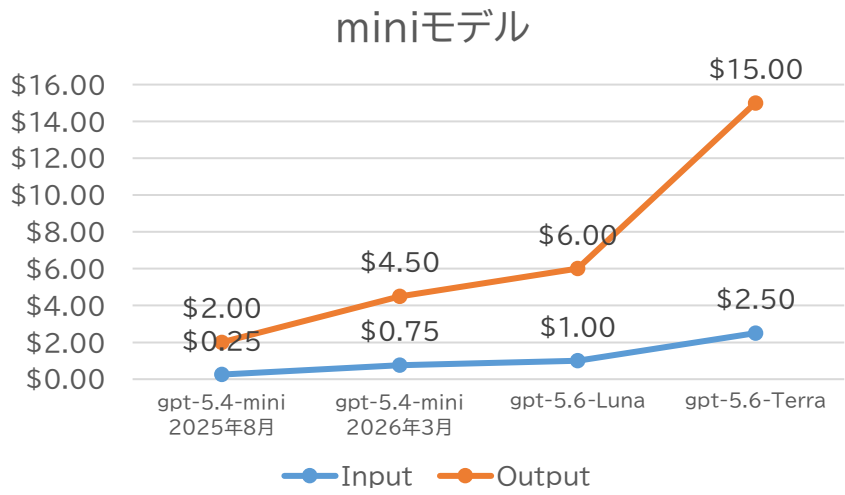
- 根本的な原因が判明しているインシデントからデータセットを構築
- 同一ログで両モデルを実行・評価
- ベンチマーク・スコアではなく：一致率、見逃し率、やり直し率等を計測
- トークン単価 vs「正しいレポートのコスト」

■ どの結果にも備える

- 精度が基準を満たす→コストはグラフのまま、削減効果は高い
- ギリギリ未達→場合によってLLMエスカレーション； 5%発生率でコストが$0.002/タスク 上がる
- 基準に届かない：APIを利用するのが正解

この先の展望





- miniモデルは～1年間で、3倍に上がっている

- 一方でオープンモデルのコスパが良くなりづつ、使いやすくなっている
- 今日の評価で勝った構成も： 明日の値上げ・提供終了で一瞬に変わりうる
- 今は精度とコストのバランスを取りづつ、価格に決断を迫られる日に向けて設計

まとめ
＋皆様とディスカッションしたい事項

まとめ・皆様とディスカッションしたい事項

① ネットワーク監視分析技術は、十分な実用段階にある

② LLMを利用するコストの削減は、最重要課題の一つ

③ 機器・トークン数だけじゃなく、申請や手続きも立派なコスト

LLMを使う際の「コスト」、何が一番困ってますか？

「解析精度」と「利用コスト」、どのように両立されていますか？

利用申請を楽にするライフハック、ありませんか？