これからのネットワーク運用に必要なデータってなんだろう？

～AIとNW運用データの「縁」～

Kohei Nishikori

Yuhei Otsuka

2025/08/01 JANOG56 in Matsue Day-3

自己紹介

Kohei Nishikori

- JANOG初参加
- 職歴: メーカー3年目
- 趣味: ロックフェス、銭湯・サウナ

Yuhei Otsuka

- 初JANOGは40福島、登壇2回目
- 職歴：NIer4年＋ISP13年 > メーカー3年目
- 趣味：ランニング、スノーボード、釣り、ワイン

Cisco CX(**C**ustomer e**X**perience) SP Japan Delivery Team

- 通信事業者向けテクニカルコンサルティングサービスを提供するチーム
- メーカーとオペレーターの両視点からオペレーションをよくするため日々奮闘中

Agenda

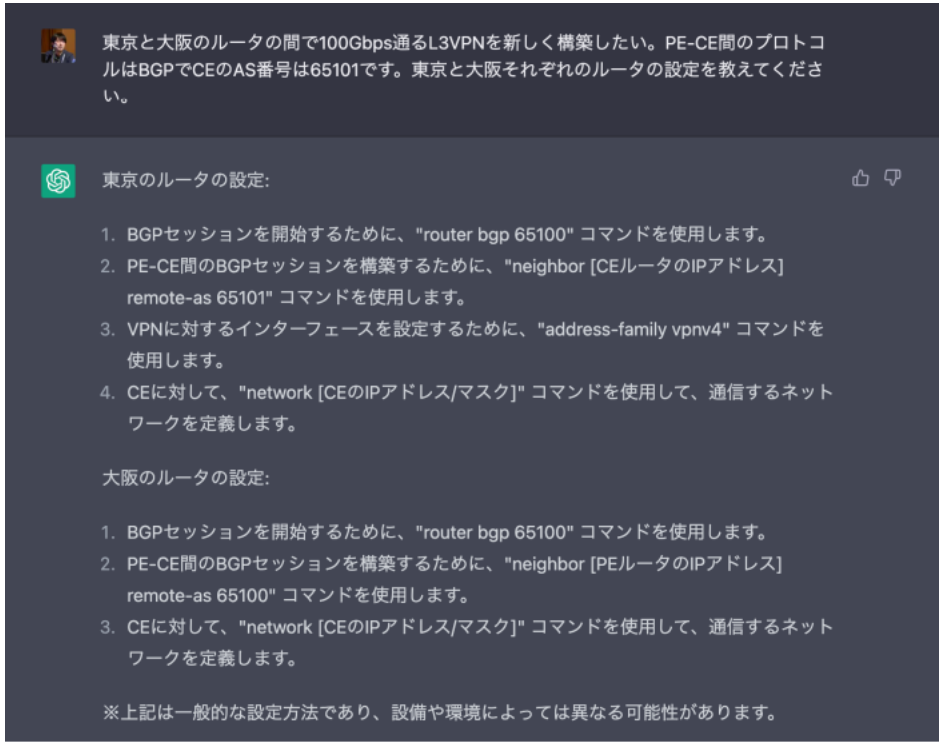
1. はじめに
2. 現在のNW運用とデータの実態
3. AI活用検討から見えてきたこと
4. 課題整理
5. 議論

JANOG の AI for Networking 議論

- 過去
  - JANOG51(2023/01) AI/MLによるネットワーク運用と自立型ネットワークに向けて
  - JANOG54(2024/07) 生成AI技術を活用したネットワークオペレーションの検討
  - JANOG55(2025/01) 生成AIによるNetwork Automation …
  - JANOG55(2025/01) レベル5 AI-NOCへの道
- JANOG56(2025/07)
  - Day-1 監視稼働削減のためのアラームコリレーションについて
  - Day-1 LLMでネットワーク構築運用支援実験@Interop Tokyo 2025 ShowNet
  - Day-2 生成AIファーストなネットワークエンジニアリングを目指して
  - Day-2 AIがどうNWの運用を変えてくれそうか？予知そして理想のダッシュボード
  - Day-2 AI AgentによるDC運用自動化の実装と課題
  - Day-3 WANネットワークにおける監視の高度化手法…
  - Day-3 「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
  - Day-3 これからのネットワーク運用に必要なデータって何だろう？　～AIと運用データの「縁」～　イマココ
  - Day-3 システム開発の常識が変わる!? ～MCPでSSoTxLLMを実現したら起きること～

ChatGPTに聞いてみた

2022末



引用元：https://www.janog.gr.jp/meeting/janog51/aiml/

2025.07

- 完全なコンフィグを出してくれるようになった！
- しかも構成図つき

ChatGPTに聞いてみた

2022末

ごめん、Juniper(JUNOS)の設定がほしい。

東京のルータの設定:

1. BGPセッションを開始するために、"set protocols bgp group external type external" コマンドを使用します。
2. PE-CE間のBGPセッションを構築するために、"set protocols bgp group external neighbor [CEルータのIPアドレス] remote-as 65101" コマンドを使用します。
3. VPNに対するインターフェースを設定するために、"set interfaces [インターフェース名] unit 0 family inet" コマンドを使用します。
4. CEに対して、"set protocols bgp group external family inet-vpn unicast prefix [CEのIPアドレス/マスク]" コマンドを使用して、通信するネットワークを定義します。

大阪のルータの設定:

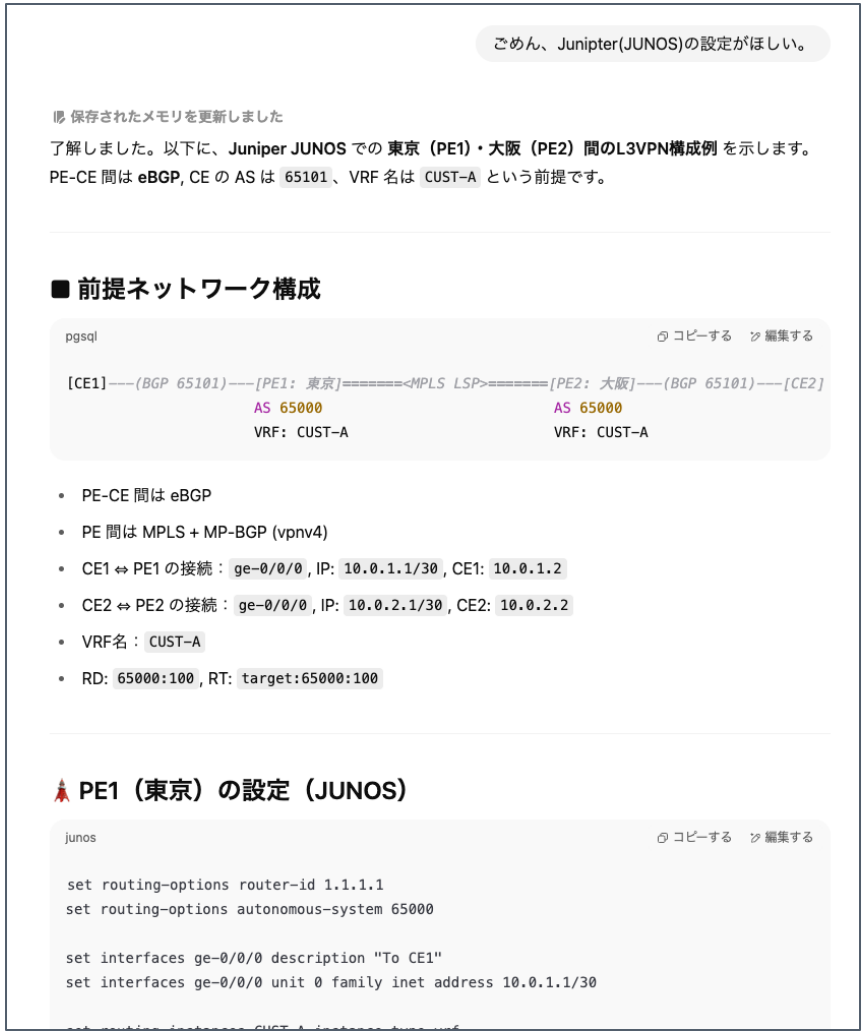
1. BGPセッションを開始するために、"set protocols bgp group external type external" コマンドを使用します。
2. PE-CE間のBGPセッションを構築するために、"set protocols bgp group external neighbor [PEルータのIPアドレス] remote-as 65100" コマンドを使用します。
3. CEに対して、"set protocols bgp group external family inet-vpn unicast prefix [CEのIPアドレス/マスク]" コマンドを使用して、通信するネットワークを定義します。

※上記は一般的な設定方法であり、設備や環境によっては異なる可能性があります。また、これらのコマンドはそれぞれの設備のJUNOSバージョンによって異なる場合がありますので、公式マニュアルを参照してください。

引用元：https://www.janog.gr.jp/meeting/janog51/aiml/

- JunOSもばっちり！

2025.07



ごめん、Junipter(JUNOS)の設定がほしい。

保存されたメモリを更新しました

了解しました。以下に、**Juniper JUNOS** での **東京（PE1）・大阪（PE2）間のL3VPN構成例** を示します。
PE-CE 間は **eBGP**, CE の AS は `65101`、VRF 名は `CUST-A` という前提です。

■ 前提ネットワーク構成

pgsql　コピーする　編集する

```
[CE1]---(BGP 65101)---[PE1: 東京]=======<MPLS LSP>=======[PE2: 大阪]---(BGP 65101)---[CE2]
                       AS 65000                            AS 65000
                       VRF: CUST-A                         VRF: CUST-A
```

- PE-CE 間は eBGP
- PE 間は MPLS + MP-BGP (vpnv4)
- CE1 ⇔ PE1 の接続：`ge-0/0/0`, IP: `10.0.1.1/30`, CE1: `10.0.1.2`
- CE2 ⇔ PE2 の接続：`ge-0/0/0`, IP: `10.0.2.1/30`, CE2: `10.0.2.2`
- VRF名：`CUST-A`
- RD: `65000:100`, RT: `target:65000:100`

PE1（東京）の設定（JUNOS）

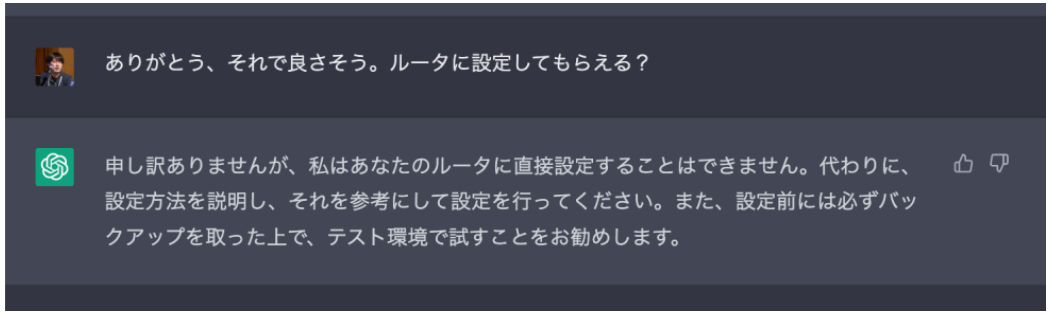
junos　コピーする　編集する

```
set routing-options router-id 1.1.1.1
set routing-options autonomous-system 65000

set interfaces ge-0/0/0 description "To CE1"
set interfaces ge-0/0/0 unit 0 family inet address 10.0.1.1/30
```

ChatGPTに聞いてみた

2022末



引用元：https://www.janog.gr.jp/meeting/janog51/aiml/

2025.07

ありがとう。それで良さそう。ルータに設定してもらえる？

どういたしまして！設定内容をご確認いただきありがとうございます。

ただし、**私は実機のルーターに直接設定を投入することはできません。**セキュリティ上、また技術的制限により、ChatGPTからネットワーク機器へアクセスしたり、設定を適用したりすることはできません。

✅代わりにできること

以下のような支援は可能です：

- **CLI投入用の設定コマンド一式をまとめる**
- **`load merge` や `commit check` などの投入方法を手順化**
- **設定投入時の注意点やロールバック手順を案内**
- **コンフィグの差分チェック用のスクリプト例を提示**
- **Junosのテンプレート化（groups構文など）**
- **ansibleやpyEZでの自動化スクリプト支援**

👇例：CLI投入の流れ（JUNOS）

bash　コピーする　編集する

```
cli
configure
load merge terminal
<ここに設定を貼り付け>
# 例:
set routing-options router-id 1.1.1.1
set routing-options autonomous-system 65000
...
<貼り付け終わったら>
Ctrl+D
commit check
commit confirmed 3
# 動作確認後に
```

- 具体的な代替案を提示してくれるようになった！

TM Forum Autonomus Network

P People(manual)　S System (autonomous)

	L0: Manual Operation & Maintenance	L1: Assisted Operation & Maintenance	L2: Partial Autonomous Network	L3: Conditional Autonomous Network	L4: High Autonomous Network	L5: Full Autonomous Network
Execution	P	P/S	S	S	S	S
Awareness	P	P	P/S	S	S	S
Analysis	P	P	P	P/S	S	S
Decision	P	P	P	P/S	S	S
Intent/ Experience	P	P	P	P	P/S	S
Applicability	N/A	Select scenario				All scenarios

	L0	L1	L2	L3	L4	L5
End-2023	9%	42%	42%	6%	1%	0%
End-2028	0%	8%	31%	44%	16%	1%

84%　Level 2 と Level 3 の間に大きな障壁　61%

Source: Capgemini Research Institute, Autonomous Telco Networks Survey December 2023–January 2024, N = 113 large CSPs link]

AN Level

ANレベル	説明	特徴
L0 – 手動運用	すべての作業を手動で実行	オフラインでの完全手動による運用・保守（O&M）
L1 – 支援付き管理	あらかじめ設定されたロジックやポリシーに基づき、一部の繰り返し作業を自動化	オンラインでの支援付き実行
L2 – 部分自律ネットワーク	ルールやポリシーに基づいて、部分的に運用・保守を自動化可能	静的なルール／ポリシーに基づく自動化
L3 – 条件付き自律ネットワーク	L2の機能に加えて、動的なルール／ポリシーに基づく自己最適化を実現	動的なルール／ポリシーに基づく自動化
L4 – 高度自律ネットワーク	L3でできることに加えて、継続的に学習可能なAI支援による自動化	継続的に学習するAI支援の自動化
L5 – 完全自律ネットワーク	最終目標 –ライフサイクル全体にわたって自律的に様々な運用を行えるシステム（人手は最小限）	自動進化、完全な自律性、あらゆるシナリオに対応。

Level4以上になると、運用ポリシーもAIが生成する

（このリンクの帯域が78Gbps以上になったら迂回する、とか）

＊ChatGPTによりベース生成

AI Agent Opsの実現例

LLMを用いて、ネットワークエンジニアの基本的なタスクを実行するためのWebアプリとAPI

ガバナンス Co-pilot
コンプライアンス Co-pilot
プランニング Co-pilot
オペレーション Co-pilot

AI エージェント

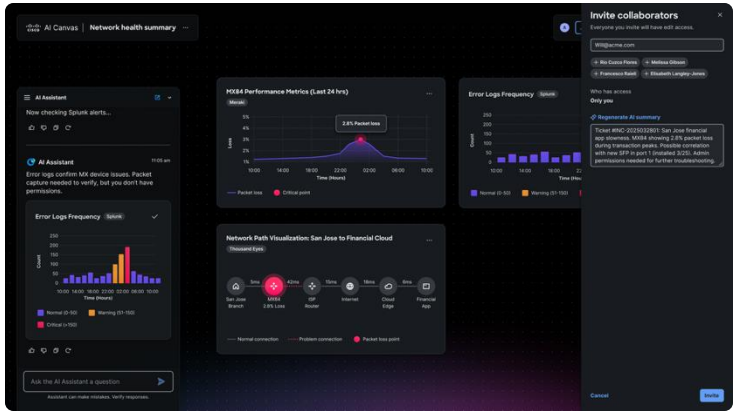
- コンフィグドリフト検知
- トラブルシューティング
- E2Eサービスアクティベーション
- ドメイン間の相関付け
- 有害因子の検出
- フォルト管理
- コンフィグ支援
- AIベースのDevSevOps
- ANレベル評価
- AI成熟度評価
- 責任のあるAI

アーキテクチャインサイト

LLM	▪ プロンプトエンジニアリング ▪ ファインチューニング ▪ RAG/ベクトルデータベース
データ収集	▪ コントローラによる統合 ▪ 顧客別データベースの構築 ▪ 文脈に沿った情報の提供 ▪ 一元的なデータ収集
UI	▪ APIを通じたアプリ統合の支援

トラブルシューティングワークフロー例

1. 自動トリガー/質問による起動
   - アラートによる自動トリガー
   - エンジニア用のインターフェースからの質問
2. トリガー/質問内容をもとに、ストアにあるワークフローに割り当てし実行
3. 実行エンジンが、保存されているテレメトリやログからデータを取得
4. 必用に応じて、ライブデータを収集するためのネットワークとのインターフェースを利用

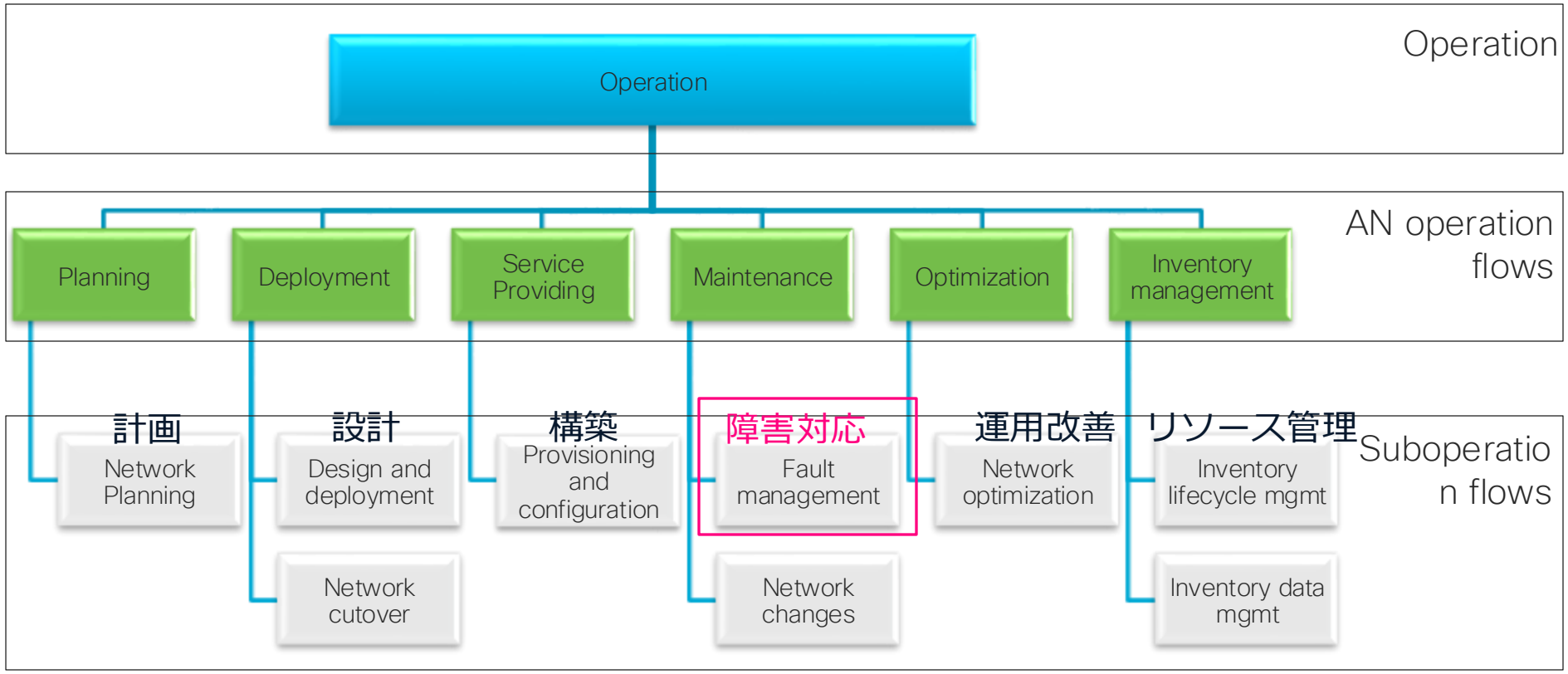


AI ダッシュボード
- オペレーターに必要な情報をAIが動的生成
- LLMを介したオペレーション
- AIエージェントによるマルチドメインネットワークおけるクローズドループの達成

とっても便利で明るい未来なんですが
AI疲れしてきませんか、、、、？

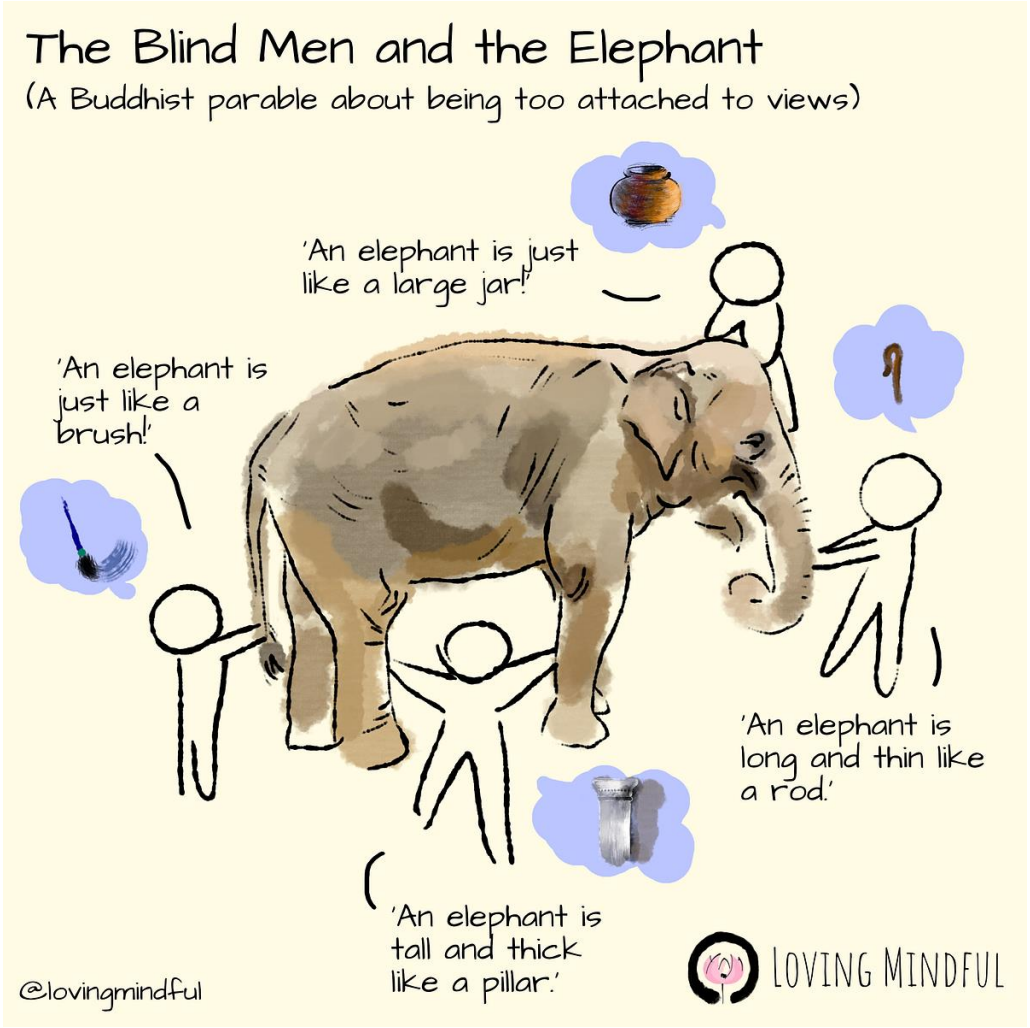
ネットワーク運用って何だ？

- ネットワークシステムやサービスを安定して稼働させるための事項、タスク
- 人の認識や状況によって定義や範囲が異なる（あるある）



参考：AN Operation Flow

データは沢山あったほうがいい？



引用元：https://sketchplanations.com/the-blind-and-the-elephant

本プログラムのサマリー

- 急速な技術進化によりNW運用においてAIが本格活用されようとしている
- JANOG56でも実装方法、分析手法・モデル、実際に商用で動かしてみたなど多数の議論があり
- 本プログラムではNW運用におけるAI活用に向けて重要となる「データ」とは何か、 今後オペレーターに求められる具体的なアクションを明確化することについて掘り下げて議論したい

今回はAN Operation Flow「Fault Management(障害対応)」を題材にしますが、もちろん他の「データ」に関する話題もWelcomeです！

議論したいこと

- 現運用ではどのようなデータを取得している？
  - ✓ そのデータによって運用者はどのような判断をしている？
  - ✓ そのデータはすぐにAIに食わせることができる？（データの非構造性、セキュリティ、データ統合/サイロ化、など）

- 今後の運用で重要なデータは何？
  - ✓RCA (Route Cause Analysis) などNW運用者の判断をAIに任せるにはどんなデータが必要？
  - ✓実際にAI運用してみて躓いたデータの課題は？（既に運用しているオペレーター向け）
  - ✓NW運用者は今後どのようなデータを取得し、AI運用に向けてどのような準備を行うべきか？

Agenda

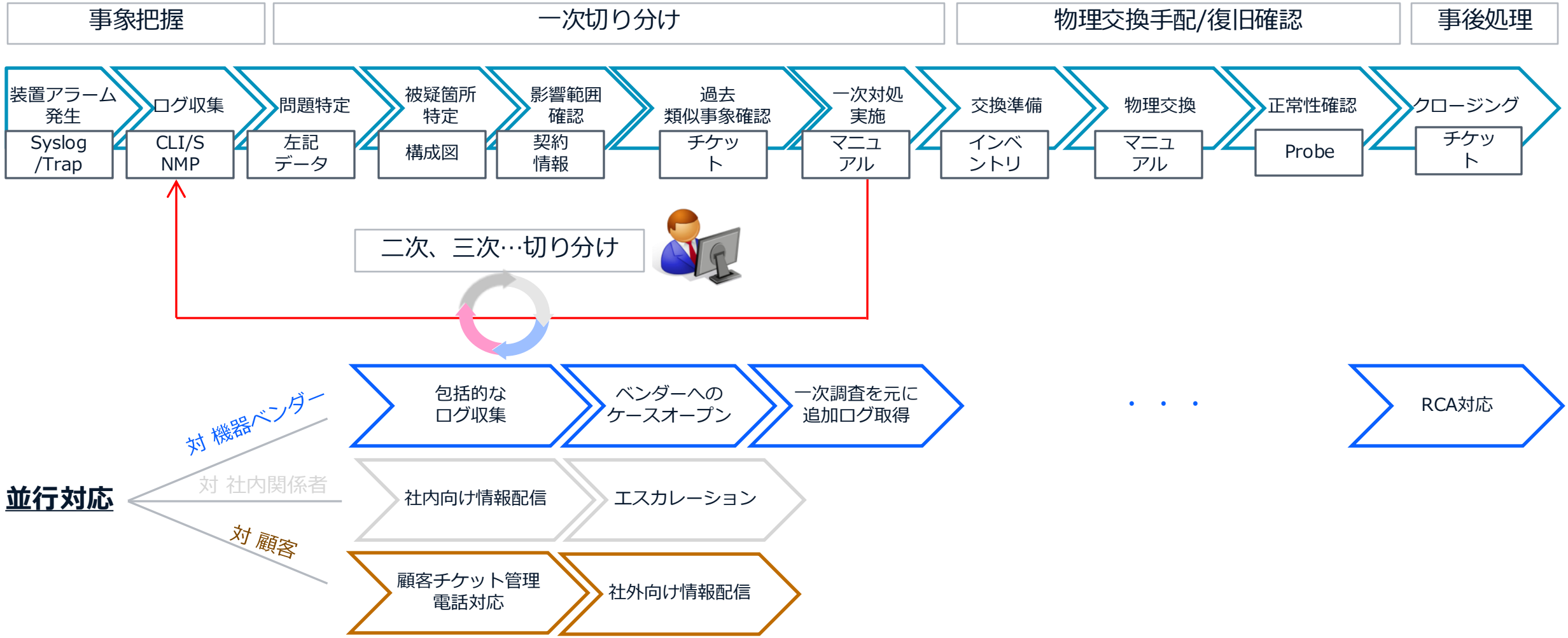
1. はじめに
2. 現在のNW運用とデータの実態
3. AI活用検討から見えてきたこと
4. 課題整理
5. 議論

NW運用に関わるデータとは？

分類	内容
可観測性データ ネットワークやシステムの状態把握、障害検知や原因分析、性能の可視化	• ログ • メトリクス • トレース
構成・リソース管理データ ネットワークの物理・論理構造やリソース割当を管理、構成変更や設計、資産管理	• インテント情報 • 機器インベントリ、コンフィグ • NWリソース、ネットワーク構成
契約・サービス情報 ネットワークとサービスの関係性把握、影響範囲の特定やサービスレベルの担保	• 契約・サービス情報 • NW機器とサービスのマッピング情報
運用履歴・チケット管理データ 運用業務に関する活動履歴、トラブル対応のトレーサビリティや改善分析	• トラブルチケット情報 • ベンダー問い合わせ履歴変更管理 • 製品ライフサイクル・不具合/脆弱性情報
マニュアル、ナレッジ 作業の標準化やノウハウを共有・蓄積するための文書・情報群	• 運用マニュアル • ベンダーマニュアル • ナレッジベース

他にも検証項目表、構築時の作業手順書・・・などなど

よくあるネットワーク運用



あらゆるタスクでデータを扱っている

運用データと判断

- 現在の運用では人がデータを確認し判断を行っている
- あるいは、事前にプリセットしたルールベースの機械的判断を行っている

障害検知

Syslog/Trap

NMSからリンクダウンアラームが発生

- ダウンしたまま→中継回線断
- 再度Upした→様子見
- リンクフラップ→SFP故障？

障害切り分け

Flow/SNMP/Telemetry

高トラフィックユーザーを特定し対処

- SNMP/Telemetryで高トラフィック自体の検出し、Src/Dst IFを特定
- Flowによってユーザー特定
- 突発かつ継続の場合、対処を検討

復旧方法決定

マニュアル、チケットデータ

どの手順を使用して復旧させるか

- 今回発生した障害は2025の8/1に発生したNWE-1234と酷似しているため、マニュアルXXXXを使用する

現状の運用データまとめ

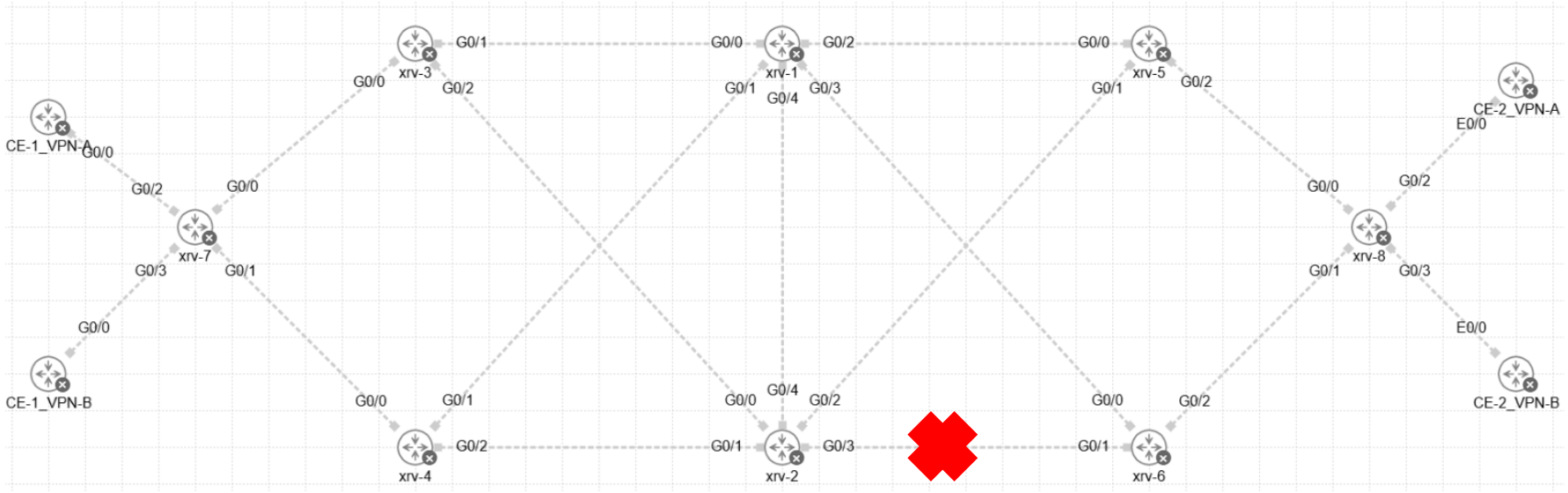
- NW運用はたくさんのデータによって支えられている
- NW運用にはたくさんのタスク（ケース）があり、それぞれにおいて必要となるデータが異なる
- NW運用では、たくさんのデータを使用しているが、多くは人の判断によるものである

Agenda

1. はじめに
2. 現在のNW運用とデータの実態
3. AI活用検討から見えてきたこと
4. 課題整理
5. 議論

実施内容サマリ

- LLM（GPT 4o）に複数パターンのデータを与え、分析をさせた結果を比較した
- その結果をもとに下記の内容について考察を実施
  1. Syslogだけのコリレーション分析と、複数の情報源（Syslog＋SNMP Trap+Topology）をもとにコリレーション分析させた場合でどのような差分が生まれる？
  2. 各社がフリーフォームで記載しているチケットデータを活用するにあたって何が情報として必要か？



1. XRv2-XRv6間でリンク断を発生させる
2. 一点時間後リンクを復旧させる
3. その間に顧客から通信断の連絡がきた場面を想定して、LLMにトラシューを実施させる

考察1
データ種類によるコリレーション分析の精度

コリレーションとは？

複数のアラートやメトリクス、ログなどの関係性を分析し、障害の根本原因や影響範囲を特定する技術

目的	具体的な目的
意味ある単位での集約	アラームではなく「インシデント（障害）」単位で把握したい
障害検知のカバレッジ拡大	今まで検知できなかった／検知しづらかった障害を把握したい
根本原因の特定（RCA）	障害のトリガーや根本原因を素早く特定したい
対応の効率化・自動化	インシデント対応の優先度判断や手順提示を支援したい
影響範囲の可視化	サービス・ユーザー・装置単位で、どこに影響が出ているか知りたい
誤検知や過検知の削減	本当に影響があるものだけを通知したい

コリレーション分析結果抜粋 (Syslogのみ)

■ 障害現象の該当機器と影響範囲の特定

- 22:00直後、以下2機器でOSPFネイバーがDOWNになっています。
  - `syc-at-sdf2-sw1` の `GigabitEthernet0/0/0/3` にて OSPFネイバー `6.6.6.6` がDOWN syslog
  - `syc-at-sdf6-sw1` の `GigabitEthernet0/0/0/1` にて OSPFネイバー `2.2.2.2` がDOWN syslog

■ 影響の継続性

- 上記OSPFネイバーは **22:02頃に再度FULL状態に復帰** しており、現時点では回復済みであると推定されます syslog 。

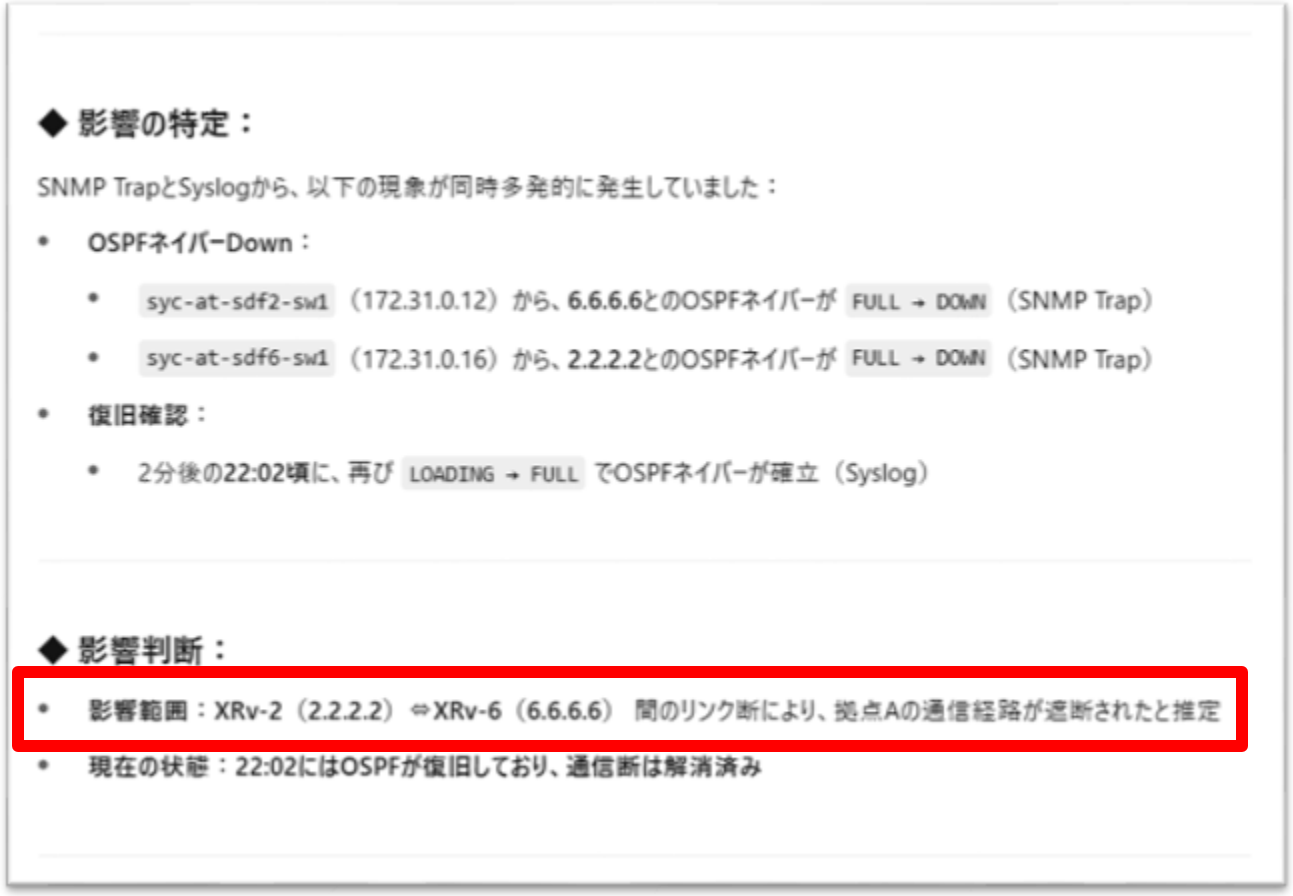
障該当機器が何で、現在はどのような状況かを分析できている

タイムライン：

時刻	イベント内容
21:59:07	syc-at-sdf2-sw1 ログイン認証失敗
21:59:39	ログイン認証成功（console）
22:00:36	syc-at-sdf2-sw1 OSPFネイバーDOWN
22:00:37	syc-at-sdf6-sw1 OSPFネイバーDOWN
22:02:10-11	両機器 OSPFネイバー復旧（FULL）
22:02:31	syc-at-sdf2-sw1 core dump発生 & devc-conaux再起動

障害と関係ない情報を含んでいるものの、Syslogから時系列に沿って情報をまとめられている

コリレーション分析結果抜粋（Syslog＋SNMPTrap+Topology）



◆ 影響の特定：

SNMP TrapとSyslogから、以下の現象が同時多発的に発生していました：

- OSPFネイバーDown：
  - `syc-at-sdf2-sw1`（172.31.0.12）から、6.6.6.6とのOSPFネイバーが `FULL → DOWN`（SNMP Trap）
  - `syc-at-sdf6-sw1`（172.31.0.16）から、2.2.2.2とのOSPFネイバーが `FULL → DOWN`（SNMP Trap）
- 復旧確認：
  - 2分後の22:02頃に、再び `LOADING → FULL` でOSPFネイバーが確立（Syslog）

◆ 影響判断：

- 影響範囲：XRv-2（2.2.2.2）⇔XRv-6（6.6.6.6） 間のリンク断により、拠点Aの通信経路が遮断されたと推定
- 現在の状態：22:02にはOSPFが復旧しており、通信断は解消済み

Topologyデータを与えることによって、具体的な障害リンクの提示ができている

考察2
チケットデータの記載方法による精度の違い

チケットデータの現状

今後AIを活用していくにあたって、社内網固有のナレッジとしてチケットデータは有用だと思われる。一方、現在のチケットデータはトラブル対応に最適化されており、暗黙の了解が多く含まれる。

＜チケット記述方法イメージ＞

チケットID: TT-20250717-005
ステータス: 対応中
優先度: 中
発生日時: 2025-07-17 18:43 JST
解決日時:
登録者: 夜勤担当（監視アラート起票）
担当者: 日勤対応へ引き継ぎ済（○○チームで対応中）

【概要】
XRv-2 ⇔ XRv-6間でリンク落ちたのが起点。複数回線に瞬断あり。OSPFも一時ダウン。

【状況メモ】
・22:01頃、サービス監視から一気に5回線分のPingアラート
・そのタイミングでXRv-2のIF（Gi0/0/0/3）がDownログ。XRv-6側も同時。

【現地対応】
・XRv-2のSFPが怪しい?（LED消灯＆リンク断継続）→ 現地にて交換依頼済
・型番は SMD

【原因判断ポイント】
・Laser Bias上がってた（DOMで確認）→ 平常時5.2mA → 9.8mA近くまで上昇
・他ポートにも同型番あり → 今後の対応必要？

【次対応】
・予防交換の方針決めたい
・OOさんには影響通知メール済（19:15送信）
・個別対応要望なし（今のところ）

【引き継ぎ】
・XRv-2に使ってるSFPの型番全体チェックしたい
・予防的な交換対象リスト作れると良さそう
・これ似た事例、7/1にもあったはず

【備考】
・取得ログ：syslog、サービス監視あり（詳しくはlogフォルダ内）

社内対応を目的として作成しているので、
人によって記載項目や記載方法に差分あり

検証チケットデータの差分

「略記を多用したフリーフォームのチケットデータ」と、「５W1Hを明確にし正確な日本語で記載したチケットデータ」で分析精度を比較。

記載方法の差分（例として一部抜粋）

略記を多用したフリーフォームのチケットデータ

【原因】
・Laser Bias上がってた（DOMで確認）→ XRv-2のSFPのDOMが5.2mA → 9.8mA近くまで上昇

５W1Hを明確にし正確な日本語で記載したチケットデータ

【原因】
分析結果:
XRv-2 側の GigabitEthernet0/0/0/3 に装着された SFP モジュールにおいて、障害発生直前のログおよび DOM（Digital Optical Monitoring）情報から、Laser Bias 電流値の異常上昇が確認された。
平常時の値（約5.2 mA）に対して、障害時は 9.8 mA を超えており、送信素子の劣化あるいは内部回路不良が疑われる状況であった。

チケットデータ分析結果

５W1Hを明確にし正確な日本語で記載したチケットデータでは下記のようなチケットデータをもとにした原因仮説と過去事例を提示できた。

原因の仮説と検証：

- 仮説：xrd-2またはxrd-6上で**一時的なプロセス異常またはSFP不調**により物理リンクが瞬断。`devc-conaux`のcore dumpや再起動が同時間帯に発生していることから、**高負荷またはプロセスクラッシュによる制御系異常**の可能性が高い。

検証のためのIOS-XRコマンド例：

bash Copy Edit

```
show interfaces GigabitEthernet0/0/0/3
show interfaces GigabitEthernet0/0/0/1
show controllers GigabitEthernet0/0/0/3
show controllers GigabitEthernet0/0/0/1
show logging
show processes cpu
show watchdog
```

過去の有効な対処例（参考）：

- 2025-07-17の障害でもSFP不良で瞬断発生→SFP交換で回復

AIが類似事象と結びつけるためには5W1Hなどを正確に記載する必要がある一方、運用者の負担は増加してしまいそう、、

見えてきたこと

検証してみてわかったこと

✓LLMによる要約ができている

- 不必要なデータも含んでしまうものの、膨大なデータを要約可能
- Syslog/Trap(テキストデータ)のみではなく、Telemetry(メトリクス)も扱えた

※多少整形が必要

✓トポロジーデータによる分析の質向上

- 単に障害が発生したことではなく、具体的に「どこ」で発生したかが分かる

✓チケットデータの中身がしっかりしてると精度が上がる

- ５W1Hが明確な文章や、必要な項目が網羅されていると精度は向上しそう
- とはいえ、実運用で項目を全て真面目に埋めるのは困難、かつ書き方にも暗黙の了解が多く含まれそう。

Agenda

1. はじめに
2. 現在のNW運用とデータの実態
3. AI活用検討から見えてきたこと
4. 課題整理
5. 議論

課題整理

課題1：目的に応じたデータ活用が必要

課題2：データ収集や活用の課題

課題3：どこまでデータ中身を綺麗にするか？

課題4：どこまでデータを貯めておくか？

（番外）LLMでどこまでメトリクスを読むか？

課題1：目的に応じて必要なデータが異なる

シーンによって必要なデータ種類は異なる

- 利用目的（検証／構築／障害対応）
- 使用者（人／AI）
- 知りたいこと（原因／影響範囲／予兆）
- タイミング（リアルタイム／後追い）
- 集め方（最低限／できる限り多く

RCA (Route Cause Analysis) などNW運用者の
判断をAIに任せるにはどんなデータが必要？

課題2：データ収集を阻む制約条件

- データがない場合、すぐに収集できるか？
  - Topology情報（特に論理）自体のモデル設計が必要
  - 既存システムへのTelemetry導入
  - Etc
- データはあっても活用しづらい
  - セキュリティの問題
- そのデータは常に更新し最新状態を維持できるか？

技術的には収集可能だが、様々な制約によって
データ収集が困難なことがある

課題3：どこまで中身を綺麗にするか？

- チケット情報などの自由記述　vs 構造化
- 自由記述をLLMで処理することの柔軟さ VS 分析精度
- 構造化されて中身のしっかりしたデータはAIにとって扱いやすいが、人間がこれを完璧に作るのは負荷が高すぎる
  - AIが使用するデータはAIが作ればよい？（チケットデータをAIで生成など）

課題4：どこまでデータを貯めておくか？

- 「とりあえず沢山とっておけ」はありか？
  - 今回検証で使用したデータは結構適当だった（データの有効性が事前にわからない状態）
    - が、簡単だが初見の問いに応えることができた
  - 人間が想像しえないことが分かるかも？
    - （今回の検証でわかったことは全て人間が想像しうることだった）
  - ただし前述の通り、収集目的や活用方法が具体的でないとデータ(宝)の持ち腐れとなる

- それとも、必要なデータに絞ってとるべきか？
  - データが増えるとコストがかかる（ストレージ領域、転送帯域、計算リソース）
  - 不要なデータ＝ノイズと化するため、学習精度が落ちる可能性あり

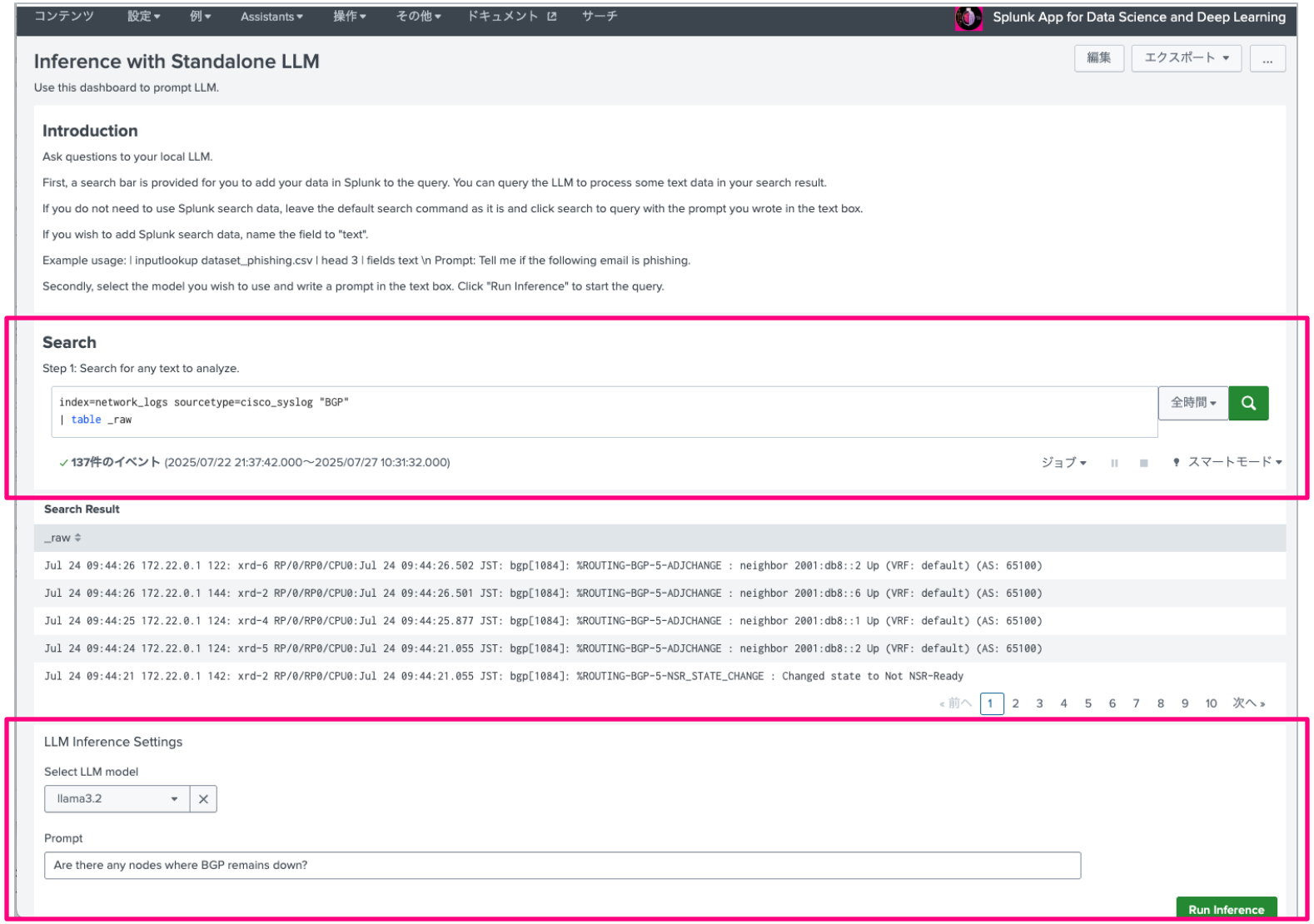
（番外）LLMでどこまでメトリクスを読むか？

従来メトリクスはML/DLでの解析が定石、今回の検証では「とりあえずLLMで」ができたが・・？

- 「とりあえずLLMで」の良さそうなところ
  - 複雑な分析をしなくてもプロンプトだけで何らかの答えを返してくれる
  - 数字に意味を持たせてくれる
  - コリレーション的に扱ってくれる

- 「とりあえずLLMで」の怪しいところ
  - 計算精度が担保されるか分からない
  - ロジックや根拠が不明確
  - 長時間など大量データの分析が困難（入力トークン制限）

こういうことができれば良いかも？（イメージ）



サーチ文でメトリクス解析してベクトル化

分析結果を含めてプロンプト入力

Agenda

1. はじめに
2. 現在のNW運用とデータの実態
3. AI活用検討から見えてきたこと
4. 課題整理
5. 議論

（再掲）議論したいこと

- 現運用ではどのようなデータを取得している？
  - そのデータによって運用者はどのような判断をしている？
  - そのデータはすぐにAIに食わせることができる？（データの非構造性、セキュリティ、データ統合/サイロ化、など）

- 今後の運用で重要なデータは何？
  - RCA (Route Cause Analysis) などNW運用者の判断をAIに任せるにはどんなデータが必要？
  - 実際にAI運用してみて躓いたデータの課題は？（既に運用しているオペレーター向け）
  - NW運用者は今後どのようなデータを取得し、AI運用に向けてどのような準備を行うべきか？

AIにはできない人間ならではの議論をしましょう！

Thank you