


セッションログを LLM で分析してみた話

株式会社ボスコ・テクノロジーズ

中山裕貴



自己紹介

- 氏名：中山裕貴
- 所属：株式会社ボスコ・テクノロジーズ
- 生息地：
 - Interop, JANOG, OOD, IEICE ICM は出没率高いです
- JANOG との関わり
 - JANOG 53 から聴講メインで参加
 - ために BoF で話したりしてます
- 普段は開発よりです（研究や運用も好きです）
 -  SMART Gateway とかを作ってます



目次

- 対象とするセッションログの紹介
- 大量のセッションログがあると直面する課題
- LLM によるセッションログの分析方法
- 実際に運用してみたの所感
- MCP と組み合わせてみた話
- まとめと今後

対象とするセッションログ

- 開発・運用・検証に関わらず、機器に接続してさまざまな操作をするかと思えます (e.g. ssh して show run).
 - このような機器に対する操作を「セッションログ」とこの発表では呼びます
 - 弊社開発している SMART Gateway を活用したら図のようなログが取れます



某幕張でもcontributionさせていただいております！

The screenshot shows a web interface for session logs. A callout box highlights the session details: user (nakayama), connection source (infra-ex2300), protocol (ssh), and user name (root). Another callout box highlights the command log table, which lists the date, protocol, destination, action, and command for each session.

日時	プロトコル	接続先	アクション	コマンド
2026/05/11 11:29:04	ssh	192.168.29.5	send	show config
2026/05/11 11:29:26	ssh	192.168.29.5	send	configure
	ssh	192.168.29.5	send	set interfaces ge-0/0/36 unit 0 family ethernet-switching vlan members development;
	ssh	192.168.29.5	send	set interfaces ge-0/0/36 unit 0 family ethernet-switching vlan members development
	ssh	192.168.29.5	send	show confi

いつどのようなコマンドを打ったかなども残る

大量のセッションログがあると直面する課題

- 埋もれます
 - 1日数百セッション全部見切るのは一苦勞です
- 本当は下記のようなことがしたい
 - 故障発生時にどのような工事が影響していそうか調査したい
 - セキュリティインシデントがあった際に、影響範囲を調べたい
 - 復旧処置としてどのようなことをしたか報告するために残したい
 - 運用時にやっていることを定型化、知識共有したい
 - and more

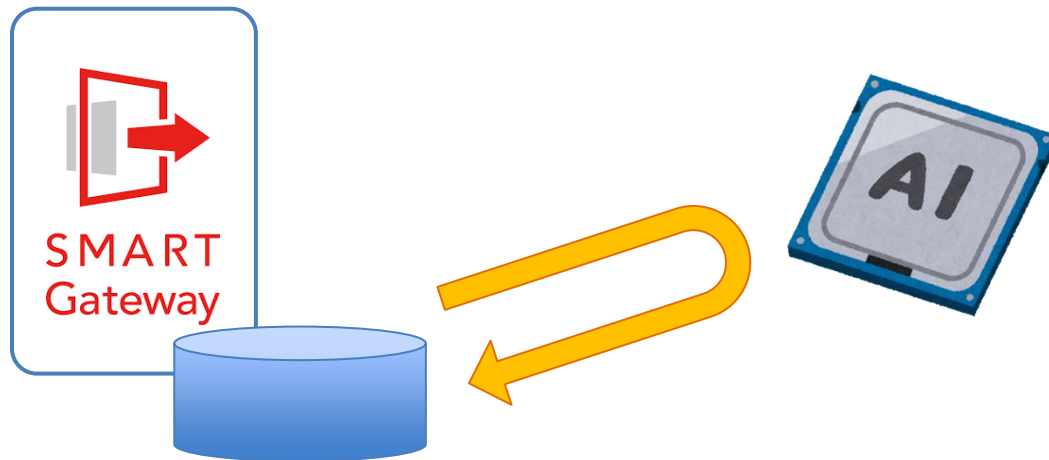


古くから AI が活躍している領域であり、
LLM 使えばきっとより楽に見るべき物を抽出できるはず！

やってみた

LLM によるセッションログの分析方法

- ポイントは大きく 2 つ
 - LLM によるセッションログのレポート化
 - 詳しくない人でもパッと概要を把握できると良し、詳しい人も詳細見ずに把握できる
 - セッションログのラベリング
 - セキュリティリスクやシステム影響度を低中高でラベリング
 - 何かあったときはそこを基本的に見れば良いはず



セッション終了段階で
・ 要約
・ ラベリング
を順次実施

host: Minisforum UM790 Pro
ollama: v0.24.0
llm model: gpt-oss:120b

実際に運用してみたの所感

• 実際に運用してみたの所感

– 結構良い

- システム影響度のラベルを眺めているだけで大体何が行われているかわかる
- ログ閲覧のみのセッションをスルーしやすくなった

– 明後日の方向のことも言うが、間違っ、影響度を低いということは少ない印象

– 案外 CPU のみでも 1 日数百セッションくらいレポートを作成してくれる

- 高価な GPU が必須ではない

セッション概要

- 接続元: 192.168.1.100 (ユーザー: nakayama)
- 接続先: 192.168.1.1 (リモートユーザー: root)
- プロトコル: SSH
- 期間: 2026/05/11 11:28:56 ~ 11:34:17

セッション レポート例

コマンド実行の流れ

1. `show config` で現在の設定を確認。
2. `configure` に入って設定モードへ遷移。
3. `set interfaces ge-0/0/36 unit 0 family ethernet-switching vlan members development;` でインタフェース `ge-0/0/36` に VLAN `development` を割り当て (2回実行)。
4. `show configuration / show interfaces` で設定反映を確認。
5. `delete interfaces ge-0/0/36 unit 0 family ethernet-switching vlan members management` により同インタフェースから VLAN `management` を除外。
6. `commit` で変更を確認。
7. `exit` を2回実行し、セッションを終了。

行動の評価

- 正規の管理者権限 (root) で実施された設定変更。
- 実行されたコマンドはすべてネットワークインタフェースの VLAN メンバーシップに関するもので、怪しい操作や不正アクセスの痕跡は見られない。
- 設定変更は単一インタフェースに限定されているが、VLAN の割り当て/除外はネットワーク分離に影響を与える可能性がある。

システム影響度	中	i
セキュリティリスク	低	i

影響度などのラベリング例

i ボタンを押すとその判定理由も見え、納得感がある

影響評価

- VLAN メンバーシップの変更は、対象インタフェース `ge-0/0/36` のトラフィックフローやネットワーク分離に直接影響を与える可能性がある。
- 変更は単一インタフェースに留まっているが、誤設定や期待外の VLAN 切り替えが発生した場合、一部システムやユーザーの接続障害が起こり得る。
- したがって、**中程度** のシステム影響と判断した。

MCP と組み合わせてみた話

- ここまで来ると MCP 化したくなる
 - やれば良いじゃない (FastMCP は偉大)

The screenshot shows a web browser window with the URL `127.0.0.1:3000/c/7d0dbdf8-56b3-4f85-abc9-4fb460b6c145`. The chat interface is titled "gpt-oss:120b".

User Query: 5/11 からどうも一部ホストと疎通が取れません。インフラで行われた工事で該当しそうなものはありますか？

AI Response: 19秒間の思考

2026年5月11日に実施された作業が原因である可能性が高いです。同日のセッションログには、以下のコマンドが実行されています。

- `set interfaces ge-0/0/36 unit 0 family ethernet-switching vlan members development` (2026/05/1111:30:14)
- 直前に `delete interfaces ge-0/0/36 unit 0 family ethernet-switching vlan members management` (2026/05/1111:31:00)

この操作により、インタフェース `ge-0/0/36` が管理 VLAN (management) から開発 VLAN (development) へ切り替えられ、管理 VLAN に属していたホストとの疎通が失われたと考えられます。

したがって、5/11以降に一部ホストと通信できなくなった問題は、上記の VLAN メンバー変更作業に起因している可能性が高いです。

*上記情報は、5/11のSSHセッション履歴から取得しています【1】。

ざっくり聞くと。。。。

欲しい結果が割と返ってくる！
ここでラベリングが効いてくる！

まとめと今後

- まとめ
 - 貯めてるセッションログ、LLM で分析すれば意外と色々捗ります。
 - MCP 化すればもっと捗ります。
 - 捗るし、シンプルに楽しいです。
- 今後
 - 定量評価したい（LLM as a Judge とか？）。
 - ただ、LLM のモデルに依存する精度評価はちょっと。。。

