G-09

アラート通知の自動識別による ネットワーク障害対応支援システムにおけるログ機能の検討

A Study of Logging Function of Network Failure Response Support System by Automatic Alert Notifications Classification

湯川 諒† 水谷 后宏‡§ 井口 信和‡§ 那須 宣亮†† 松山 浩士††

Ryo Yukawa Kimihiro Mizutani Nobukazu Iguchi Nobuaki Nasu Koji Matsuyama

1. 序論

令和2年度に総務省が実施した調査によると電気通信サービスの事故発生状況は 6610 件であり前年度より 4.9%増加している [1]．また，令和 3 年度の調査では 6696 件と，ほぼ横這いになっている．その一方で，重大な事故は 7 件と前年度より 3 件増加している．電気通信サービスの重大な事故とは，影響利用者数が 3 万人以上又は継続時間が 2 時間以上の事故と定義され，令和元年度以降，増加傾向となっている [2]．

昨今のネットワーク障害は，ネットワーク自体が社会基盤となっていることから迅速な復旧が必要とされる [3]．また，ネットワークの集中化が進むとされる一方で，ネットワークエンジニアの人手不足が深刻化し，ネットワーク障害時に実施するトラブルシューティングの負担が増大していくと予想される．そのため，高度化・複雑化するネットワークシステムに対して，運用保守作業の強化が求められている [4]．

しかし現状のネットワーク監視ツールの多くは，障害を検知すると些細な事象でもアラートを通知する設定となっている．その結果，ネットワークエンジニアは，アラート通知の確認に追われるため，トラブル推定への遅れが発生し，障害対応が後手になる可能性がある．

そこで本研究では，24 時間 365 日対応のネットワーク運用保守業務に焦点を当て，アラート通知の自動識別を目的に，機械学習を用いて，アラート通知を解析する機能を開発する．さらに，トラブル推定するネットワークエンジニアの障害対応における作業負担の軽減を目的に，ネットワーク障害対応支援システム(以下，本システム)を開発する．本システムでは，アラート通知の障害対応表(以下，対応表)を基に，「アラート通知分類用 AI モデル(以下，分類用 AI モデル)」と「トラブル対応推論用 AI モデル(以下，推論用 AI モデル)」を各サーバに用意する．そして，クライアント PC からの障害の対応内容の要求に対する対応策を自動応答する．AI モデルを 2 つに分けることで精度を高めることが期待できる．本システムにより，大量のアラート通知からのトラブルを推定する手間が省け，トラブルシューティングの負担軽減が期待できる．本稿では，現在までに実装した機能と実装予定のログ機能について述べる．

†近畿大学大学院 総合理工学研究科, Graduate School of Science and Engineering, Kindai University

‡近畿大学 情報学部, Faculty of Informatics, Kindai University

§近畿大学 情報学研究所, Cyber Informatics Research Institute, Kindai University

††株式会社サイバーリンクス, CYBERLINKS CO.,LTD.

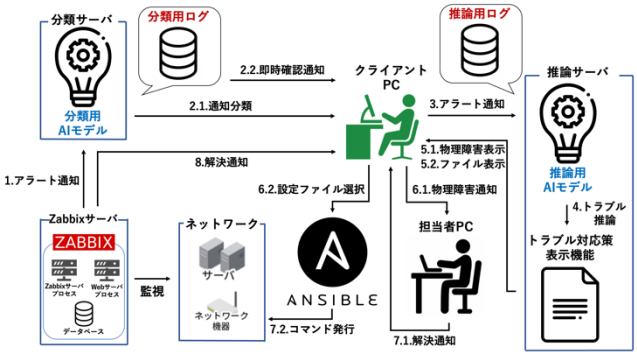

図 1　システム構成図

2. 関連研究・関連サービス

関連研究として紅林らの研究[5]がある．紅林らの研究では，論理型言語 Prolog でルールを記述し，知識ベースに基づく 2 段階のトラブル推論で原因を推定するネットワークトラブルシューティングの自動化が可能である．一方で，本研究では，PyTorch でニューラルネットワークを構築し，アラート通知の事前分類とトラブル対応の推論が可能である．また，トラブル推論後にトラブル対応策の提案が可能である．

関連サービスとして IIJ 統合運用管理サービス for ZABBIX[6]がある．IIJ 統合運用管理サービスでは，確認すべきアラート通知のみを抽出し，対応の必要なアラート通知はチケット管理システムに自動登録する．それゆえ，Zabbix から送られてくる大量アラート通知をフィルターで自動削減することが可能である．一方で，本研究では，Zabbix のアラート通知の対応表で作成した推論用 AI モデルでトラブル対応の推論が可能である．また，トラブル推論後にトラブル対応策の提案が可能である．

3. 研究内容

3.1. システム概要

本システムの構成を図 1 に示す. 本システムはクライアントプログラムとサーバサイドプログラムから構成される. クライアントプログラムは, 対応の必要なアラート通知やトラブル対応策の表示をサーバサイドプログラムに要求する. サーバサイドプログラムは, アラート通知分類機能・トラブル対応推論機能・トラブル対応策表示機能を有しており, 分類用 AI モデルと推論用 AI モデルを動作させる.

3.2. 本システムの機能

サーバサイドプログラムに実装した三つの機能の概要と新たに実装予定のログ機能について述べる.

3.2.1. アラート通知分類機能

本機能は, アラート通知を分類する機能である. 分類項目は, 「確認の必要な通知」, 「対応の必要な通知」, 「対応と確認が不要な通知」の 3 つである. 分類用 AI モデルは, Zabbix サーバから送られてきたアラート通知を入力とし, 確認の必要な通知・対応の必要な通知を出力する. 入力したアラート通知は, Bag of Words モデル・TF-IDF モデルで数値化している. 本機能により, アラート通知をあらかじめ分類し, 必要な通知のみを送信することで迅速な対応が可能である.

3.2.2. トラブル対応推論機能

本機能は, 対応の必要なアラート通知のトラブル対応を推論する機能である. 推論用 AI モデルは, 対応の必要なアラート通知を入力とし, 推論したトラブル対応を出力する. 入力したアラート通知は, Bag of Words モデル・TF-IDF モデルで数値化している. トラブル対応は, 現時点で 18 種類設定しており, 入力のアラート通知に最も該当するものを出力する. 本機能により, 機器の種類やホスト名に対してトラブル対応を推論することでネットワークエンジニアの分析判断の支援が可能となる.

3.2.3. トラブル対応策表示機能

本機能は, 推論用 AI モデルで出力したトラブル対応から対応策を生成して表示する機能である. 提案できるトラブル対応策は, 物理障害連絡先の提案と Ansible で用いる PlayBook ファイルの提案である. 本機能により, トラブルシューティング時に対応策を確認でき, 円滑にトラブル対応に当たることが可能となる.

3.2.4. ログ機能

本機能は, 分類用ログ機能と推論用ログ機能で構成される. 分類用ログ機能の役割は「ログ取得」, 「ログ通知」の 2 つであり, 推論用ログ機能の役割は「ログ取得」である.

分類用ログ機能のログ取得は, 分類サーバによるアラート通知の自動識別処理のログを取得する機能である. 本機能により, アラート通知の識別結果を可視化でき, ネットワーク運用保守作業のトラブル推定に役立てることが期待できる.

分類用ログ機能のログ通知は, 分類サーバのアラート通知分類機能を補完する機能である. 現状の分類用 AI モデルは, 大量のアラート通知をフィルタリングすることで, ネットワークエンジニアの作業負担を軽減することが期待できる. しかし, 分類サーバのフィルタリングに誤りがあった場合, 必要なアラート通知がフィルターを通過できないという問題点がある. これにより, 必要なアラート通知が対応されずに放置され, ネットワーク運用保守作業における重要な障害の見逃しにつながる. この問題の対応策として, Zabbix の繰り返し通知を併用することで, 同一の内容のアラート通知のログを短時間で 2 回取得した場合, 必要なアラート通知を不要なアラート通知と誤って分類したと判断する. その後, 分類用ログ機能を利用することで, 必要なアラート通知をクライアント PC へ即時確認すべき通知として送信する. 本機能により, ネットワーク運用保守作業における必要なアラート通知の見逃しを防ぐことが可能である.

推論用ログ機能のログ取得は, 分類用ログ機能のログ取得と同様に推論サーバによるアラート通知の自動識別処理のログを取得する機能である. 本機能により, アラート通知の識別結果を可視化でき, ネットワーク運用保守作業のトラブル推定に役立てることが期待できる.

4. 結論

本研究では, 24 時間 365 日対応のネットワーク運用保守業務に焦点を当て, アラート通知の自動識別を目的に, 機械学習を用いて, アラート通知を解析する機能を開発している. さらに, トラブル推定するネットワークエンジニアの障害対応における作業負担の軽減を目的に, ネットワーク障害対応支援システムを開発している. 本システムでは, AI モデルの精度を高めることを目的に, AI モデルを 2 つ利用する. この利点として, 大量のアラート通知を事前分類し, 対応の必要なアラート通知のトラブル対応を推論することが可能である. 本システムを利用することで, 24 時間 365 日対応のネットワーク運用保守業務のアラート通知からトラブルを推定する手間が省け, トラブルシューティングの負担軽減が期待できる. 今後, 本システムにログ機能を実装する予定である.

参考文献

1) 総務省：電気通信サービスの事故発生状況（令和 2 年度）, 入手先〈https://www.soumu.go.jp/main_content/000770066.pdf〉(参照 2023-7-7) .
2) 総務省：電気通信サービスの事故発生状況（令和 3 年度）, 入手先〈https://www.soumu.go.jp/main_content/000845066.pdf〉(参照 2023-7-7) .
3) 金井俊介, 浅井文香, 村田尚美ほか：機械学習を使ったネットワーク障害箇所学習プロセス, 電子情報通信学会論文誌 B, Vol.J104-B, No.3, pp.163-174 (2021) .
4) JST-CRDS：研究開発の俯瞰報告書｜システム・情報科学技術分野 (2023), 入手先〈https://www.jst.go.jp/crds/pdf/2022/FR/CRDS-FY2022-FR-04/CRDS-FY2022-FR-04_20607.pdf〉(参照 2023-7-7) .
5) 紅林輝, 梶克彦, 河口信夫：知識ベースに基づくネットワークトラブルシューティングの自動化, インターネットコンファレンス論文集 2010, 25-26 Oct 2010.Tokyo.Japan.65-72 (2010)
6) 「-IIJ 統合運用管理サービス for ZABBIX-」で面倒なアラート処理を自動化, 入手先 〈https://www.iij.ad.jp/svcsol/campaign/uom_201802.html〉(参照 2023-7-7).