2ZB-01

アラート通知自動識別による ネットワーク障害対応支援システムのログ機能の実装

湯川 諒† 水谷 后宏‡§ 井口 信和‡§ 那須 宣亮†† 松山 浩士††

近畿大学大学院総合理工学研究科† 近畿大学情報学部‡

近畿大学情報学研究所§ 株式会社サイバーリンクス††

1. 序論

令和 3 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 6709 件であり前年度と比較するとほぼ横這いになっている[1]. しかし，令和 4 年度の調査では 7500 件と，大幅に増加している．また，重大な事故は 10 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．

また現状のデータセンターは，ネットワークシステムの高度化・複雑化に伴い，技術的に複雑化している．その結果，故障箇所を特定する判断に時間がかかっている．

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

†Ryo YUKAWA, Graduate School of Science and Engineering, Kindai University

‡Kimihiro MIZUTANI, Nobukazu IGUCHI, Faculty of Informatics, Kindai University

§Kimihiro MIZUTANI, Nobukazu IGUCHI, Cyber Informatics Research Institute, Kindai University

††Nobuaki NASU, Koji MATSUYAMA, CYBERLINKS CO.,LTD.

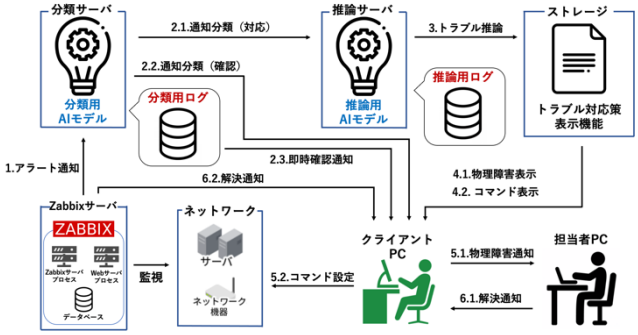

図 1 システム構成図

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と迅速な分析判断を目的に，ネットワーク障害対応支援システム(以下，本システム)を開発している[5]．本システムでは，アラート通知情報と障害対応表(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)」を各サーバに用意し，アラート通知を自動識別する．AI モデルを 2 つに分けることで 1 つの時よりも、アラート通知の識別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とアラート通知の迅速な分析判断が期待できる．本稿では，実装内容を変更したトラブル対応策表示機能と新たに実装したログ機能について述べる．

2. 研究内容

2.1. 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 Gmail とサーバサイドスクリプトから構成される．サーバサイドスクリプトは，Gmail が受信したアラート通知を識別するための AI モデルが付与されたアラート通知分類機能・トラブル対応推論機能を有している．また，本システムに必要な処理をするトラブル対応策表示機能・ログ機能を有している．

2.2. 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コマンド設定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できる．

2.3. 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「アラート通知のログ取得」，「ログ通知」の 2 つであり，推論用ログ機能の役割は「対応の必要な通知のログ取得」である．

分類用ログ機能のアラート通知のログ取得は，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．

推論用ログ機能の対応の必要な通知のログ取得は，分類用ログ機能のアラート通知のログ取得と同様に推論サーバによる対応の必要な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，対応の必要な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．

分類用ログ機能のアラート通知のログ取得の可視化した例を図 2 と図 3 に示す．図 2 は，1 時間毎のアラート通知数を棒グラフで示し，図 3 は，図 2 の 8 時間分のアラート通知の識別結果を円グラフで示す．

3. 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

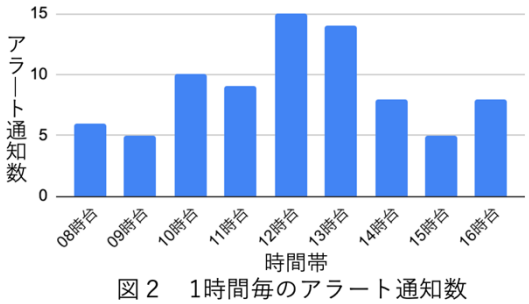

図 2 1時間毎のアラート通知数

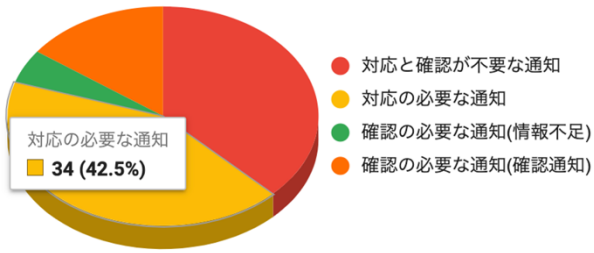

図 3 8時間分のアラート通知の識別結果

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と迅速な分析判断を目的に，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とアラート通知の迅速な分析判断が期待できる．また，本システムにログ機能を実装したことで，アラート通知の識別結果を可視化し，ネットワーク運用保守作業における「確認と対応が必要なアラート通知」の見逃しの防止が期待できる．

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 3 年度），入手先〈https://www.soumu.go.jp/main_content/000897411.pdf〉（参照 2023-12-19）．
2) 総務省：電気通信サービスの事故発生状況（令和 4 年度），入手先〈https://www.soumu.go.jp/main_content/000897675.pdf〉（参照 2023-12-19）．
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) 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）
5) 湯川諒．“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.” 2023 年度 情報処理学会関西支部 支部大会 講演論文集 2023（2023）．