C-21

トラフィックとフローに基づいたネットワーク運用管理システム TRAFL の機能拡張

Extension of the network operation management system "TRAFL" based on the traffic and the flow

陰地　健太†　　川橋　裕‡

Kagechi Kenta　　Kawahashi Yutaka

1.　はじめに

災害や障害時の被害を最小限に，局所化する対応力のあるネットワークを構築するためには，管理者が監視するネットワークと，外部との通信記録を正確に把握する必要がある．したがって，障害原因の究明および対応をおこなうためには，ネットワークの運用管理を支援するシステムが必要となる．和歌山大学で運用している TRAFL[1]は，ネットワーク境界部の通信記録を保持しているシステムである．保存した通信記録をグラフとして表示することで，視覚的に通信状況を把握できる．しかし，Web ブラウザで表示される要素が限られた情報のみであり，過去の通信記録を参照する場合，データベースに SQL やコマンドを入力する必要があるため，管理者の負担が大きく，調査に時間を要する．

本研究では，上記の問題を解決するため，検索機能を備えた Web ユーザインタフェースを実装し，障害対応にかかる利便性の向上を目標とする．

2.　先行研究

TRAFL はネットワークサイド，サーバサイド，ユーザサイドの 3 つの構成から成り立っている．システム構成を図.1 に示す．ネットワークサイドでは，ネットワーク境界部に設置したスイッチのポートミラーリング機能を利用し，サーバサイドにパケットを送信している．ポートミラーリング機能とは，あるポートが送受信するデータを，同時にポートミラーリング設定したポートへデータを送出する機能である．この機能を用いることで，ネットワーク境界部の通信を取得できる．また，ポートミラーリング機能を利用することで，TRAFL のシステムに障害が発生し，TRAFL の機能が停止した場合でも，ネットワークサイドの通信の妨げにならないため，組織内ネットワークの保守性を高めている．サーバサイドでは，パケットキャプチャにより取得したデータをフロー形式でデータベースに保存する．本システムでは，IP ヘッダの情報である送信元 IP アドレス・送信元ポート番号・宛先 IP アドレス・宛先ポート番号が全て一致するパケット群をフローと定義した．データベースに保存された情報を基に，グラフやランキング形式に加工し，Web ブラウザで表示させることで，管理者は時間毎のトラフィックの詳細な記録を表示でき，ネットワークの状況を確認するのが容易になる．

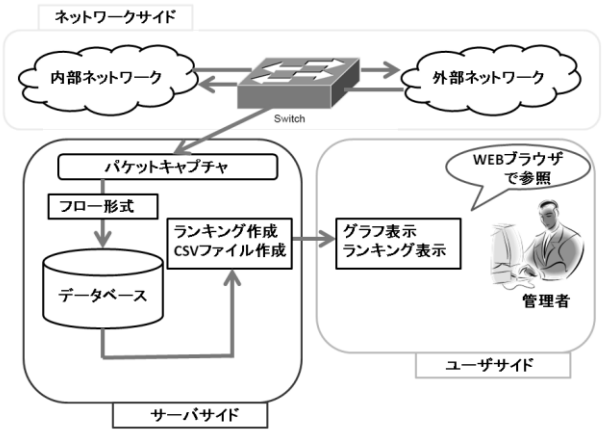


図 1.TRAFL のシステム構成

3.　研究目的

従来の TRAFL では，以下の問題点が挙げられる．

- DB 検索の手順が多く，管理者の負担が大きい．
- 特定のポート番号以外のグラフ表示不可能．
- グラフ表示できる期間は本日・前日のみ

そこで，本研究では，TRAFL の Web ユーザインタフェースを作成し，利便性の向上を図ることで，管理者の負担を軽減させることを目的とする．具体的には，Web ユーザインタフェースに検索したい項目を入力することで，コマンドや SQL を入力する手順を省略しデータベース検索を可能にする．加えて，従来の TRAFL では表示できない IP アドレスやポート番号ごとのグラフ，ランキング表示を可能とし，過去 1 カ月に遡りグラフを出力できるシステムの作成をおこなう．

4.　提案手法・システム

本研究では，データベース検索をおこなう Web ユーザインタフェースを作成する．通信記録の調査を支援するために，以下の項目をデータベース検索の条件に指定できるようにした．

- パケットタイプ
- パケット方向
- IP アドレス
- ポート番号
- 時刻
- ランキング種類
- データベース検索・グラフ出力

†和歌山大学大学院, Graduate School of Systems Engineering, Wakayama University
‡和歌山大学システム情報学センター ,Center for Information Science, Wakayama University

提案システムの構成を図.2 に示す．既存の TRAFL のシステム構成に加えて，ユーザサイドに，提案手法のデータベース検索をおこなう Web ユーザインタフェースを作成した．実装した Web ユーザインタフェースを図.3 に示す．本システムにより，ネットワーク管理者が WEB ユーザ インタフェースに検索条件を入力することで，入力された情報をもとに SQL やコマンドを作成しデータベースの検索やグラフの出力をおこなう．検索結果の一例を以下に示す．図.4 はインタフェースに検索条件を入力しており，UDP 通信における，外部ネットワークから内部ネットワークへの通信(ここでは，Incoming とする)の，トラフィックランキングを表示する．その検索結果が図.5 である．

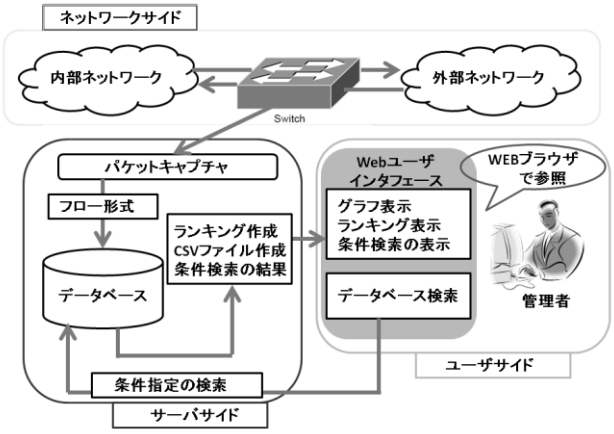


図 2.提案システムの構成図

図 3.Web ユーザインタフェース

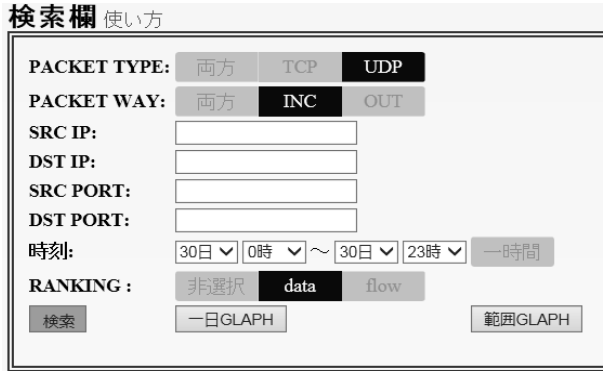
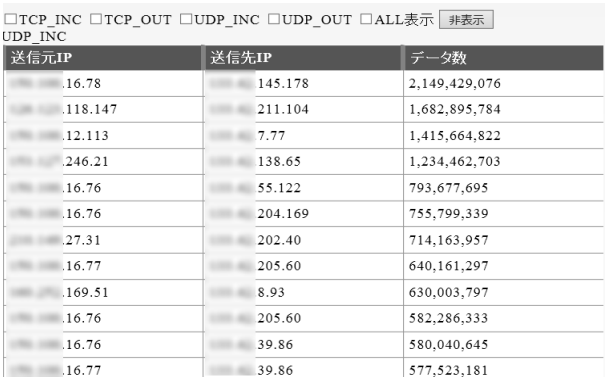


図 4. 検索条件:UDP 通信・Incoming・30 日 0 時～24 時 データランキング



□TCP_INC □TCP_OUT □UDP_INC □UDP_OUT □ALL表示 非表示

UDP_INC

送信元IP	送信先IP	データ数
.16.78	145.178	2,149,429,076
.118.147	211.104	1,682,895,784
.12.113	7.77	1,415,664,822
.246.21	138.65	1,234,462,703
.16.76	55.122	793,677,695
.16.76	204.169	755,799,339
.27.31	202.40	714,163,957
.16.77	205.60	640,161,297
.169.51	8.93	630,003,797
.16.76	205.60	582,286,333
.16.76	39.86	580,040,645
.16.77	39.86	577,523,181

図 5. 検索結果:UDP 通信・Incoming・30 日 0 時～24 時 データランキング

5. 実験

提案システムを用いて，Web ユーザインタフェースで管理者がネットワークの異常を発見できるか実験をおこなった．本実験では，NTP を利用したDDoS 攻撃を被害者用端末におこなう．本実験は，2017 年2 月17 日の8 時00 分から23 時00 までの期間でおこなった．従来のTRAFLであれば，グラフ表示により，トラフィックが急激に増加している時間帯を把握し，一時間毎にどの端末が一番多く通信していたかを把握出来たが，どのような通信が行われていたかを確認するためにはデータベースに接続し，確認を取る必要があった．また，長い期間におけるランキングを表示する事が不可能であった．提案手法では，Webユーザインタフェースに期間，通信相手や通信元のIPアドレス・ポート番号を指定する事で，特定の端末が，どのような通信で，どの頻度でやり取りされているかを全てWebブラウザ上ですぐに確認する事が可能となる．これにより，管理者が詳細なデータを閲覧するためにサーバに接続する必要がなくなり，特徴のある通信を発見しやすくなり，負担が削減されたといえる．

6. 評価

本章では，5 章で述べた実験の結果をもとに，実装したシステムの評価と考察を行う．

6.1 従来の TRAFL との比較評価

提案システムでは，管理者の負担を減らすために，TRAFLのWeb ユーザインタフェースを作成することにより，Webブラウザでデータベース検索を可能にした．また，IP アドレス，ポート番号を指定することで，特定の通信端末，通信プロトコルのトラフィックグラフの表示を可能にし，障害原因の局所化が可能になると考える．加えて，過去1ヶ月のトラフィック・フロー数におけるグラフ表示をおこなうことで，通信記録を後から参照することが容易になる．以上のことから，提案システムは既存のTRAFL と比較して，データベース検索における管理者の負担を抑えることができ，円滑な障害調査がおこなえるといえる．

6.2 今後の課題

本節では，本研究で構築したTRAFLの今後の課題について述べる．

6.2.1 データベース検索処理の向上

長期間におけるTRAFLのデータベース検索をおこなった際，複数のデータベース内のテーブルから，検索条件に一致する値を取得する．加えて，グラフやランキング表示の

場合には取得した値をそれぞれ加工する必要がある．そのため，データベース検索結果の表示に必要な時間が大きく，円滑な通信記録の調査を妨げている．データベース検索結果の表示に必要な時間を短縮するためには，データベース検索時に使用するプログラムの改善をおこなう必要があると考える．

6.2.2　監視するパケット情報の追加

TRAFLのデータベースに保存されるパケット情報は宛先IP アドレス，宛先ポート番号，送信元IP アドレス，送信元ポート番号，時刻，ヘッダ長である．しかし，パケット情報には端末同士の通信接続の確立に利用される制御ビットや，通信状態を確認するために用いられる情報があり，それらの情報をデータベースに追加することで，通信状況の把握や障害調査が容易になると考えている．

7. おわりに

本研究では，管理者の負担を軽減するために，TRAFLのWebユーザインタフェースを作成し，Web ブラウザでデータベース検索を可能にした．データベース検索に必要なSQL やコマンドの入力を省略することで，障害調査を円滑におこなうことができる．加えて，Web ユーザインタフェースにIP アドレスやポート番号を指定することで，端末やプロトコル毎のランキング，トラフィックグラフを把握できるため，障害の局所化が可能となり，障害調査が容易になると考える．今後は，データベース検索に必要な時間を短縮し，表示できるパケット情報の種類を増やすことで，管理者が障害調査を円滑におこなえるように，システムを改良していきたい．

参考文献

[1] 釼本　倫章　”トラフィックグラフとフローに基づくネットワーク管理支援システムTRAFL の構築と運用″
2015 年度修士論文,和歌山大学大学院システム工学研究科
[2]小原　康平　“宛先ポート番号別グラフを用いたトラフィックデータ参照システム”
2014年度卒業論文，和歌山大学システム工学部情報通信システム学科
[3]井尾　明日香　“グラフを用いたトラフィックデータ参照システム”
2011年度卒業論分，和歌山大学システム工学部情報通信システム学科
[4] 経済産業省
″「情報セキュリティ総合戦略」の概要″
http://www.meti.go.jp/policy/netsecurity/downloadfiles/Strategy_Summary.pdf
[5] ″MRTG::The Multi Router Traffic Grapher″
http://www.mrtg.jp/doc/
[6] ″Wireshark″
https://www.wireshark.org/