1W-05

複数の拠点を接続するネットワーク構成に対応したネットワークトラフィック可視化システムの検討

波々伯部勇貴† 井口信和‡

近畿大学大学院総合理工学研究科† 近畿大学理工学部情報学科‡

1. 序論

地理的に離れた複数の拠点を持つ組織では，インターネット上で VPN 等を用いて，拠点間を相互に接続する．例えば，企業の本店と支店間や，大学の本部キャンパスと地方キャンパス間の通信などがある．組織内のネットワーク管理者は，これらのネットワークのセキュリティを確保するため，監視や統計情報の収集などを専用のシステムを導入して実施している[1]．ネットワーク監視を行うためのシステムの一つにネットワークトラフィック可視化システムがある[2-3]．このシステムの多くは，予め作図ソフトでネットワークの論理構成図を作成し，図上のネットワーク機器に対して IP アドレスの対応付けを行う必要がある．また，通信を監視するための専用機器を購入する必要があるため導入コストが高くなる．そのため，中小企業などの組織では，ネットワーク管理者の知識不足や予算不足などの問題によって導入が難しい場合がある．

そこで，当研究室ではネットワークの状況を素早く把握することを目的に，小規模企業のネットワーク管理を対象とする，トラフィック可視化システム（以下，既存システム）を開発してきた．既存システムはゲームエンジンである Unity により開発した．既存システムでは，一台のルータが送受信した通信パケットだけしか再現できない．そのため，複数のルータを有するネットワーク構成に対応できないという問題がある．

そこで本研究では，複数の拠点を接続するネットワーク構成に対応したネットワークトラフィック可視化システム（以下，本システム）の検討を行う．本システムは，既存システムを基盤技術として使用し，新たに実装する．本システムは簡便に使用できることを目的に，通信パケットからネットワークの論理構成を自動的に再現し，さらにネットワークトラフィックを可視化する．そのため，ネットワークの論理構成図を予め作成する必要がない．また，通信パケットの記録を用いるため，通信を監視するための専用機器を購入する必要がない．本システムは複数の通信パケットの記録を読み込み可能とするように実装する．これにより複数のルータを接続するネットワーク構成の再現が可能となる．本システムにより，ネットワーク管理者はネットワークの状況を簡便に可視化できる．

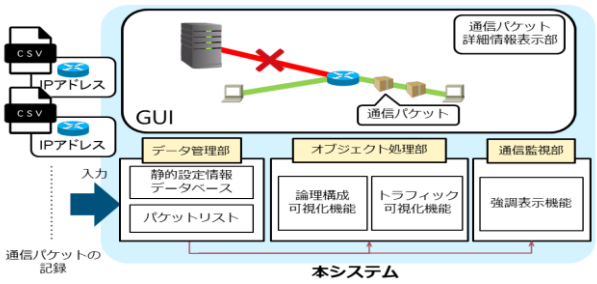

図 1：システム構成図

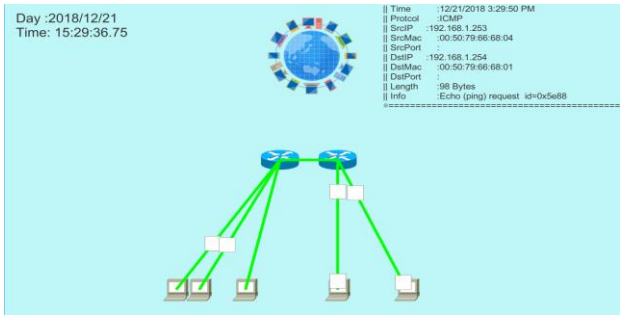

図 2：GUI

2. 検討システム

本システムの構成を図 1 に示す．本システムはそれぞれのルータで収集した通信パケットを csv 形式で保存したものを入力として扱う．csv ファイルごとに収集を行ったルータの IP アドレスを付加することにより，そのルータが送受信した通信パケットをパケットリストに格納する．また静的設定情報データベースはルータ，サーバ，プリンタなどの機器の IP アドレスを保管す

Study on Network Traffic Visualization System Corresponding to Network Configuration Connection Multiple Sites
†Yuki HOKABE, Graduate School of Science and Engineering Research, Kindai University
‡Nobukazu IGUCHI, Department of Informatics, Faculty of Science and Engineering, Kindai University

る．これらのデータをオブジェクト処理部，通信監視部が随時参照する．各機能の処理結果は図 2 の GUI に出力する．通信パケット詳細情報表示部は時刻や送信元・宛先 IP アドレスなどの通信パケットの詳細情報を表示する．

本システムの要件は，ネットワークの論理構成とトラフィックの可視化及び通信の疎通状況を直感的に把握可能にすることである．要件を達成するためのアプローチとして，通信パケットの記録から LAN・拠点間ネットワークの論理構成とトラフィックを可視化することでネットワークの状況を再現する．また，可視化されたネットワーク機器間のリンクを通信の疎通状況に応じて色分けることで強調する．以下に，それぞれの機能の詳細について述べる．

2.1 論理構成可視化機能

本機能では，収集した通信パケットからネットワークの論理構成を可視化する．本機能は監視対象のネットワークに存在する機器の IP アドレスを静的設定情報データベースに予め登録しておくことにより，自動的にノードの種類を識別する．まず，パケットリストから送信元または宛先のプライベート IP アドレスをすべて抽出する．次に，抽出した IP アドレスを用いて，静的設定情報データベースを検索する．静的設定情報データベースにその IP アドレスが登録されている場合，そのノードのオブジェクトを生成する．該当しない場合は，ホスト PC のオブジェクトを生成する．さらに，生成したノードのオブジェクトに IP アドレスを紐付ける．最後にオブジェクト処理部が各ノード間のリンクを構成する．それらを基にネットワークの論理構成を GUI 上に表示する．本機能により，ネットワークの論理構成を可視化する．

2.2 トラフィック可視化機能

本機能では，通信パケットの流れを時系列順にアニメーションを用いて可視化する．本機能はパケットリストにある通信パケットごとの時刻情報に基づいて，プロトコル別に色分けられたオブジェクトを生成する．まず，送信元・宛先アドレスの情報から通信パケット毎にアニメーションの始点と終点の座標を決定する．次に，収集を行ったルータの IP アドレスを用いて，アニメーションの中継点の座標を決定する．アニメーションは通信パケットオブジェクトの各生成タイミングと同時に再生する．本機能により，トラフィックを可視化する．

2.3 強調表示機能

本機能では，ノード間のリンクを通信の疎通状況に応じて色を分けて強調表示する．通信監視部は各リンク上に流れる通信パケットを監視し，次の通信パケットが流れるまでの時間を計測する．その計測時間が 60 秒を経過するとリンクを緑色から灰色に色分けする．ホストとルータ間では，計測時間が 300 秒を経過するとリンクを消去する．本機能により，通信の疎通状況を直感的に把握できる．

3. 実験・考察

実験では，動作検証と性能評価実験を行う予定である．

動作検証では，本システムが要件を満たすかを確認する．まず，検証のために，ネットワークシミュレータを用いて，様々な論理構成のネットワークを構築する．次に，構築したネットワークにて様々な通信を行い，その通信パケットを収集する．最後に収集した通信パケットを本システムに入力する．以上により収集した通信パケットから，ネットワークの論理構成とトラフィックが可視化されることを確認する．また，ノード間のリンクを通信の疎通状況に応じて色を分けて強調表示されることを確認する．

性能評価実験では，本システムにおけるオブジェクトの描画数に応じた CPU 使用率と描画処理が完了するまでの時間を計測する．これにより，複数の拠点を接続するネットワーク構成に対応できるかどうかを確認する．

4. 結論

本研究では，複数の拠点を接続するネットワーク構成に対応したネットワークトラフィック可視化システムの検討を行った．本システムは複数の通信パケットの記録の読み込み可能とするように実装する．これにより複数のルータを接続するネットワーク構成の再現が可能となる．本システムにより，ネットワーク管理者はネットワークの状況を簡便に可視化できる．今後は動作検証および性能評価実験を実施する予定である．

参考文献

1) IT 人材育成本部 産学連携推進センター：ネットワーク管理に関する知識，情報処理推進機構（オンライン），入手先<https://www.ipa.go.jp/files/000056032.pdf>，(参照 2018-12-25).
2) 鈴木宏栄，衛藤将史：実ネットワークトラフィック可視化システム NIRVANA の開発と評価，情報通信研究機構季報, Vol.57，No.3，pp. 63-80(2011).
3) 脇村亜衣，青木茂樹，宮本貴朗：組織内ネットワークのトラフィックの可視化と異常検出支援ツールの開発，研究報告インターネットと運用技術（IOT），Vol.40，No32，PP1-8(2018).